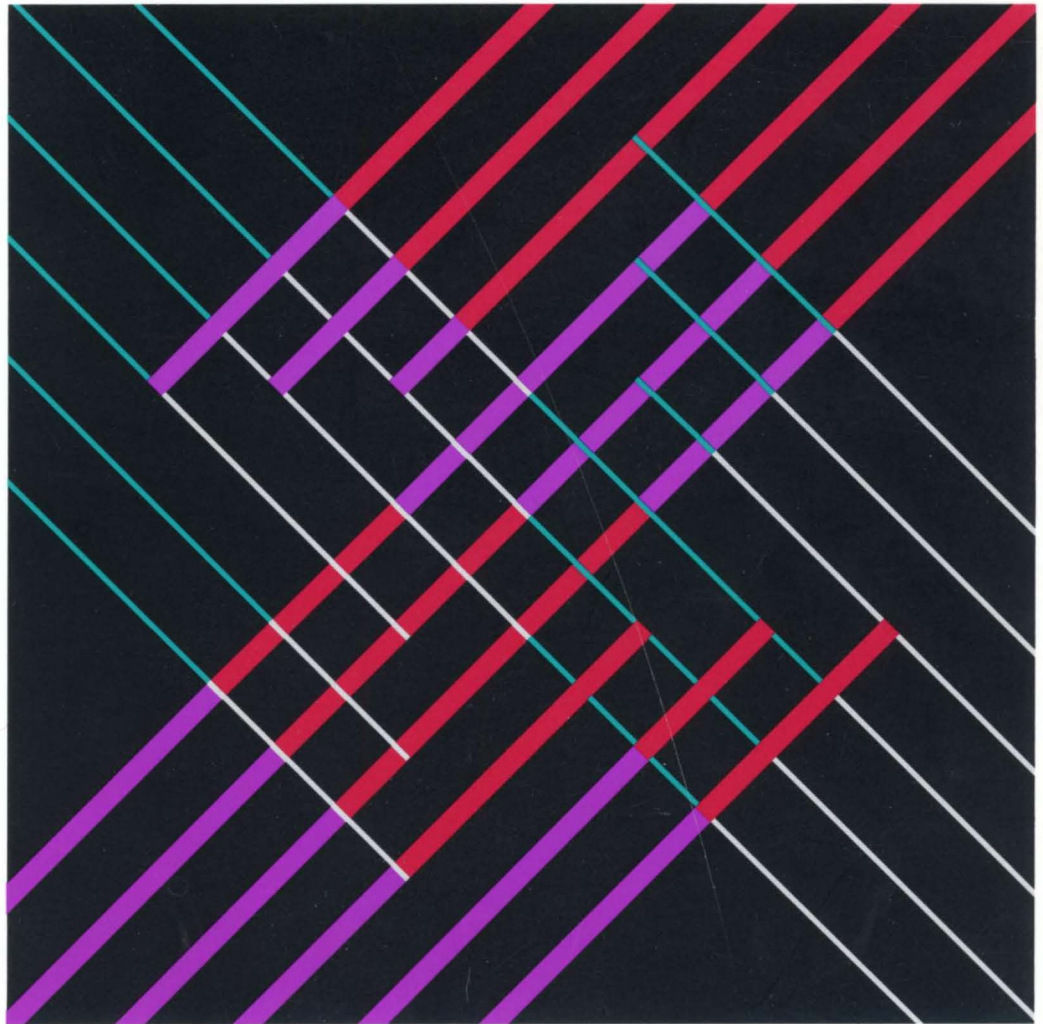


Multiprotocol Network Program

SC30-3559-02

User's Guide Version 1 Release 1.1 and Version 1 Release 1.2





Multiprotocol Network Program

SC30-3559-02

User's Guide Version 1 Release 1.1 and Version 1 Release 1.2

Third Edition (May 1993)

Note

Before using this information and the product it supports, be sure to read the general information under "Notices" on page xxiii.

This is the third edition of the *IBM Multiprotocol Network Program User's Guide*. This edition applies to Version 1 Release 1.1 and Version 1 Release 1.2. of the IBM Multiprotocol Network Program and to all subsequent releases and modifications until otherwise indicated in new editions.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

Forms for readers' comments are provided at the front and back of this publication. If the forms have been removed, address your comments to:

IBM Corporation
Department E15
P.O. Box 12195
Research Triangle Park, North Carolina 27709-9990
U.S.A.

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 1992, 1993. All rights reserved.

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	xxiii
Trademarks	xxiii
 About This Book	xxv
Summary of Changes	xxvi
Who Should Use This Book	xxvi
IBM 6611 and Multiprotocol Network Program Libraries	xxvii

Part I: Using the Configuration Program

Chapter 1. Preparing for Configuration	1-1
About this Chapter	1-2
Getting Started	1-3
Configuration Considerations	1-10
General Recommendations for Configuration	1-10
Changing Configuration Parameters	1-11
 Chapter 2. Using the Configuration Program	2-1
Introduction to the Configuration Program	2-2
Using the Configuration Program on a RISC System/6000 Workstation	2-3
Hardware and Software Requirements	2-3
Installing the Configuration Program	2-3
Starting the Configuration Program	2-4
Using the Configuration Program on a PS/2 Workstation	2-5
Hardware and Software Requirements	2-5
Installing the Configuration Program	2-5
Starting the Configuration Program	2-6
Operating the Configuration Program	2-6
The Main Window	2-7
The Menu Bar	2-9
Creating an IBM 6611 Configuration File	2-9
Transporting the Configuration File to the IBM 6611	2-13
Transporting the File Using a Diskette	2-13
Transporting the File without Using a Diskette	2-13
 Chapter 3. System Configuration Parameters	3-1
About this Chapter	3-3
Source Route Bridging	3-4
Spanning Tree Parameters	3-5
Port Filter Order	3-6
Transparent Bridging	3-10
Filtering Database Parameters	3-12
Spanning Tree Parameters	3-16
Data Link Switching	3-18
Systems Network Architecture (SNA)	3-27
SNA Frame Filters	3-27
Advanced Peer-to-Peer Networking	3-32
Configuring an IBM 6611 Network Node	3-32
Network Node Configuration	3-34
Data Link Switching Connection	3-36
IP Connection	3-41

Tuning an IBM 6611 Network Node	3-43
NetBIOS	3-47
NetBIOS Name Filters	3-48
IP Routing Protocols	3-51
Routing Information Protocol	3-58
Hello Protocol	3-63
Border Gateway Protocol (BGP)	3-67
BGP Global Default Parameters	3-67
BGP Group Parameters	3-69
BGP Neighbor Parameters	3-73
BGP Import Filters	3-77
Exterior Gateway Protocol (EGP)	3-83
Static Routes	3-90
Packet Filters	3-92
Route Exports	3-95
IP over X.25	3-100
AppleTalk	3-101
Enabling the AppleTalk Protocol	3-101
Internet Packet Exchange (IPX)	3-102
Xerox Networking System (XNS)	3-109
DECnet	3-115
 Chapter 4. System Management Parameters	 4-1
About this Chapter	4-2
IBM 6611 Names	4-3
EIA 232 Serial Ports	4-4
Lock or Unlock the Multiprotocol Network Program	4-5
Simple Network Management Protocol	4-6
Userids and Passwords	4-16
Configuration Hosts	4-18
Time to Perform Configuration	4-19
Remote Host Names	4-21
Name Servers	4-22
Time Servers	4-23
 Chapter 5. Adapter Configuration Parameters	 5-1
About this Chapter	5-2
Token-Ring Network 16/4 Adapter	5-3
Ethernet Adapter	5-6
EIA 422/449 Serial Adapter and V.35/V.36 Serial Adapter	5-9
LAN Bridging Protocol	5-12
Point-to-Point Protocol (PPP)	5-16
Frame Relay	5-18
SDLC Adapter	5-21
SDLC Adapter SNA Stations	5-25
X.25 Adapter	5-30
 Chapter 6. Protocol Configuration Parameters	 6-1
About this Chapter	6-3
Which Protocols Does Each Adapter Support?	6-4
Source Route Bridging Port Parameters	6-5
Source Route Bridge Filters	6-8
Defining the Order of Port Filters	6-8
Inbound MAC Address Filters	6-9
Inbound Source SAP Filters	6-10
Inbound SNAP Value Filters	6-11

Inbound Ring Number Filters	6-12
Inbound Sliding Window Filters	6-13
Inbound Filter Order	6-16
Outbound MAC Address Filters	6-18
Outbound Source SAP Filters	6-20
Outbound SNAP Value Filters	6-21
Outbound Ring Number Filters	6-22
Outbound Sliding Window Filters	6-23
Outbound Filter Order	6-25
Hop Count Filter	6-27
Transparent Bridging Port Parameters	6-29
Transparent Bridge Filters	6-32
Defining the Order of Port Filters	6-32
Maximum Transmission Unit Size	6-33
Inbound MAC Address Filters	6-33
Inbound Source SAP Filters	6-35
Inbound Ethernet Type Filters	6-36
Inbound Sliding Window Filters	6-37
Inbound Filter Order	6-39
Outbound MAC Address Filters	6-41
Outbound Source SAP Filters	6-43
Outbound Ethernet Type Filters	6-43
Outbound Sliding Window Filters	6-45
Outbound Filter Order	6-47
SNA Port Parameters	6-49
NetBIOS Port Parameters	6-50
IP Port Parameters	6-51
IP Port Filters	6-52
IP Destinations Per DLCI	6-55
AppleTalk Port Parameters	6-57
Network Number Ranges	6-57
AppleTalk Ports	6-57
Network Zone Lists	6-57
AppleTalk Port Filters	6-58
User Restrictions on Routing	6-58
Configuration Options	6-58
Define Port Characteristics	6-60
Define Additional Zone Names for Network Zone List	6-62
Define AppleTalk Filters for the Port	6-62
Define DLCI Numbers for Frame Relay Connection	6-64
Restrict Routing to Selected Networks Only	6-64
List of Selected Networks	6-65
IPX Protocol Port Parameters	6-68
XNS Port Parameters	6-75
DECnet Port Parameters	6-82

Part II: Using the System Manager

Chapter 7. Operating the System Manager	7-1
Introduction to System Manager	7-2
Using the System Manager Screens	7-3
Menu Screens	7-4
Selector Screens	7-6
Dialog Screens	7-7
Command Status Screens	7-9

Using the Function Keys in the System Manager	7-11
Making Selections from a List of Choices	7-13
Getting System Manager Help	7-14
Contextual Help	7-14
General Help	7-14
Performing System Manager Tasks	7-16
Flowchart of System Manager Menu Screens	7-17
Performance and Statistics	7-22
Problem Determination Facilities	7-23
Concurrent Hardware Diagnostics	7-25
Resource Control and Management	7-27
System Environment and Configuration	7-28
Remote Accesses to Other Nodes	7-30
Software Installation and Maintenance	7-31
Hardware Vital Product Data	7-34
Configuration Files and Reports	7-35
Adapter and Protocol Configuration	7-36
 Chapter 8. Using the Fast-Path Environment and Command Primitives	 8-1
Introduction	8-6
Executing the Command Primitives	8-6
Accessing the Fast-Path Environment	8-7
Exiting the Fast-Path Environment	8-7
Getting Help in the Fast-Path Environment	8-8
Adapter Debug Facility Command Primitives	8-10
adp_dump	8-10
adp_line_trc_start	8-10
adp_name_list	8-10
adp_read_mem	8-11
adp_show_regs	8-11
Address Resolution Protocol: Adapter Command Primitives	8-12
aarp_adp_list	8-12
arp_adp_add_perm_nopub	8-12
arp_adp_add_perm_pub	8-12
arp_adp_add_temp_nopub	8-13
arp_adp_add_temp_pub	8-13
arp_adp_del_addr	8-13
arp_adp_del_host	8-14
arp_adp_flush	8-14
arp_adp_list	8-14
interface_list	8-15
Address Resolution Protocol: System Command Primitives	8-16
arp_hw_type_list	8-16
arp_sys_add_perm_nopub	8-16
arp_sys_add_perm_pub	8-16
arp_sys_add_temp_nopub	8-17
arp_sys_add_temp_pub	8-17
arp_sys_del_host	8-17
arp_sys_list	8-18
Bridging Debug Facility Command Primitives	8-19
brdg_cfg_info	8-19
brdg_sap_filter	8-19
port_list	8-19
stat_adp_brdg	8-20
stat_adp_lanbr	8-20
stat_srb_sptree	8-20

stat_srb_sptree_frm	8-21
stat_sys_lanbr	8-21
stat_sys_lanbr_frm	8-21
stat_tb_sptree	8-22
stat_tb_sptree_frm	8-22
trace_brdg_start	8-22
trace_brdg_stop	8-23
trace_brdg_view	8-24
Configuration Command Primitives	8-25
config_app	8-25
config_com	8-25
config_err_rpt	8-25
config_file_run	8-26
config_list	8-26
config_reinstate	8-26
config_rej	8-27
config_rpt	8-27
config_script	8-27
config_sysid	8-28
DECnet Debug Facility Command Primitives	8-29
dec_adj	8-29
dec_area_cost	8-29
dec_area_hop	8-30
dec_area_min_cost	8-30
dec_area_min_hop	8-31
dec_area_out_adj	8-31
dec_area_reach	8-32
dec_circuit	8-32
dec_cost	8-33
dec_executor	8-33
dec_hop	8-33
dec_min_cost	8-34
dec_min_hop	8-34
dec_out_adj	8-34
dec_reach	8-35
trace_dec_level	8-35
trace_dec_log	8-36
trace_dec_mask	8-36
trace_dec_time	8-36
Diskette Command Primitives	8-37
disk_dwn_files_dos	8-37
disk_dwn_files_unix	8-37
disk_format_dos_hi	8-37
disk_format_dos_low	8-38
disk_format_unix_hi	8-38
disk_format_unix_low	8-38
disk_list_files_dos	8-38
disk_list_files_unix	8-39
disk_up_files_dos	8-39
disk_up_files_unix	8-39
Dump: System Command Primitives	8-40
dump_ex_err_log	8-40
dump_ex_trc_log	8-40
dump_prev_info	8-40
dump_system	8-40
dump_system_format	8-41

dump_system_trans	8-41
Dump: User Process Command Primitives	8-42
dump_appn	8-42
dump_ipproto	8-42
dump_process	8-42
proc_list	8-42
Error Report Command Primitives	8-43
err_id_list	8-43
err_log_trans	8-43
err_rpt_det	8-43
err_rpt_eid_det	8-44
err_rpt_eid_sum	8-44
err_rpt_etype_det	8-45
err_rpt_etype_sum	8-45
err_rpt_hw_det	8-46
err_rpt_hw_rsc_det	8-46
err_rpt_hw_rsc_sum	8-47
err_rpt_hw_sum	8-47
err_rpt_op_det	8-48
err_rpt_op_sum	8-48
err_rpt_seq	8-49
err_rpt_sum	8-49
err_rpt_sw_det	8-49
err_rpt_sw_rsc_det	8-50
err_rpt_sw_rsc_sum	8-50
err_rpt_sw_sum	8-51
err_type_list	8-51
hw_rsc_list	8-52
seq_num_list	8-52
sw_rsc_list	8-52
Fast-Path Environment Exit Commands	8-53
exit	8-53
quit	8-53
File Management Command Primitives	8-54
files_clr_all_trans	8-54
files_clr_one_trans	8-54
files_list_static	8-54
files_list_trans	8-55
files_rename_trans	8-55
files_view_static	8-55
files_view_trans	8-56
Hardware Command Primitives	8-57
hw_cfg_chg	8-57
hw_def_list	8-57
hw_detail	8-57
hw_diag	8-57
hw_diag_list	8-58
hw_install_list	8-58
hw_serial_model	8-58
hw_sup_list	8-59
hw_vpd_list	8-59
Host Name Command Primitives	8-60
host_name_set	8-60
host_name_show	8-60
Host Name to IP Address Mapping Command Primitives	8-61
map_host_add	8-61

map_host_del	8-61
map_host_list	8-61
Install Command Primitives	8-62
install_cleanup	8-62
install_comp	8-62
install_fix_list	8-62
install_not_commit_list	8-63
install_reinstate_saved_comp	8-63
install_remove_saved_comp	8-63
install_sw_list	8-63
install_up_trans	8-64
install_upd	8-64
install_upd_commit	8-64
install_upd_reject	8-64
install_verify	8-65
Name Server Command Primitives	8-66
name_serv_add	8-66
name_serv_del	8-66
name_serv_list	8-66
name_serv_start	8-67
name_serv_stop	8-67
Process Command Primitives	8-68
proc_command	8-68
proc_info	8-68
proc_list	8-68
proc_stat	8-68
proc_table	8-69
Remote Access Commands	8-70
atecho	8-70
ftp	8-70
modem_rcv	8-70
modem_send	8-71
ping	8-71
rlogin	8-71
telnet	8-72
Route Table Command Primitives	8-73
interface_list	8-73
route_adp_table	8-73
route_sys_table	8-73
Serial Port Command Primitives	8-74
modem_rcv	8-74
modem_send	8-74
s1_at	8-74
s1_baud	8-75
s2_at	8-75
s2_baud	8-75
Shutdown: System Command Primitives	8-76
shutdown_at_ipl	8-76
shutdown_at_noipl	8-76
shutdown_soon_ipl	8-76
shutdown_soon_noipl	8-77
Software Lock Primitive	8-78
sw_lock	8-78
Software VPD Command Primitives	8-79
sw_dep_list	8-79
sw_files_list	8-79

sw_history	8-79
sw_id	8-79
sw_list	8-80
sw_prereq	8-80
sw_upd_list	8-80
Statistic-Gathering Command Primitives	8-81
interface_list	8-81
stat_adp_con	8-81
stat_adp_filter	8-81
stat_adp_pack_traf	8-81
stat_adp_proto	8-82
stat_adp_proto_mon	8-82
stat_inet	8-82
stat_io	8-83
stat_mem_man	8-83
stat_net_con	8-83
stat_route	8-83
stat_socket	8-84
stat_sys_activity	8-84
stat_sys_pack_traf	8-84
stat_sys_proto	8-85
stat_virt_mem	8-85
Terminal Control Primitives	8-86
set_backspace	8-86
set_interrupt	8-86
Time Server Command Primitives	8-87
time_serv_add	8-87
time_serv_del	8-87
time_serv_list	8-87
time_serv_start	8-88
time_serv_stop	8-88
Time: System Command Primitives	8-89
time_date_set	8-89
time_zone_set	8-89
Trace: System Command Primitives	8-91
trace_grp_list	8-91
trace_grp_start	8-91
trace_id_list	8-91
trace_id_start	8-91
trace_log_trans	8-92
trace_rpt_all	8-92
trace_rpt_id	8-92
trace_stop	8-93
Trace: User Process Command Primitives	8-94
trace_appletk_parm_list	8-94
trace_appletk_start	8-94
trace_appletk_stop	8-94
trace_appn_parm_list	8-94
trace_appn_set_flags	8-95
trace_appn_stop	8-95
trace_iproto_parm_list	8-95
trace_iproto_start	8-95
trace_iproto_stop	8-96
trace_snmp_list	8-96
trace_snmp_start	8-96
trace_snmp_stop	8-96

trace_sys_man_trans	8-97
User: System Command Primitives	8-98
user_add	8-98
user_del	8-98
user_list	8-98
user_passwd	8-99
3-Digit Display Command Primitive	8-100
read_3digit	8-100
 Chapter 9. Accessing the IBM 6611	9-1
About This Chapter	9-2
Local Access Configurations	9-2
Stand-Alone IBM 6611	9-2
Direct-Attached Terminal	9-3
Remote Access Configurations	9-4
Network-Attached Terminal	9-4
Modem-Attached Terminal	9-5
Extended Network Configurations	9-6
Accessing a Local IBM 6611	9-6
Accessing a Remote IBM 6611	9-7
Using an IP Network Connection	9-7
Using a Modem	9-17
Accessing the IBM 6611 through the EIA 232 Serial Ports	9-19
General Setup Attributes	9-19
Communication Setup Attributes	9-20
Transferring Files with Serial Port Access	9-23
Logging In to an IBM 6611	9-23
Userids and Passwords	9-25
Controlling User Tasks	9-25
 Chapter 10. Operating the IBM 6611	10-1
About This Chapter	10-3
Performing Resource Control and Management Tasks	10-3
Starting the IBM 6611	10-4
Stopping the IBM 6611	10-4
Reading the Three-Digit Display	10-6
Viewing the System Route Table	10-7
Viewing the Adapter Route Tables	10-9
Viewing the Network Management Subsystem Information	10-11
Managing ARP Tables	10-13
Viewing Adapter AARP Entries	10-17
Exporting the Route Table Information	10-18
Performing System Environment and Configuration Tasks	10-18
Working with Files in the Transfer Directory	10-19
Viewing a File in the Static Directory	10-21
Sending an AT Command to a Modem Attached to an EIA 232 Serial Port	10-22
Performing Diskette Operations	10-22
Showing and Changing the Date and Time	10-26
Changing the Date, Time, and Time Zone	10-27
Performing System Configuration Changes	10-28
Transferring Files	10-43
File Names for Output in Transfer Directory	10-43
Exporting Specific Data	10-50
Importing Specific Data	10-51
Exporting Files to a Remote Node	10-52
Importing Files from a Remote Node	10-52

Using the File Transfer Protocol	10-52
Using the Xmodem Protocol	10-55
Transferring Files to Diskette	10-57
Selling the IBM 6611 to a Third Party	10-57
Chapter 11. Problem Determination	11-1
About This Chapter	11-3
Problem Determination Facilities Provided by the System Manager	11-3
Selecting a Problem Determination Facility	11-3
Using the IBM 6611 Problem Determination Facilities	11-3
Error Log Facility Overview	11-4
View an Error Report	11-6
View an Error Report for a Single Sequence Number	11-8
Clean the Error Log	11-10
Use System and User Process Dump Facilities	11-11
Use System Trace Facility	11-21
Use Special User Process Traces	11-24
Use Adapter Debug Facility	11-37
Use Source Route Bridging Debug Facility	11-42
Use DECnet Debug Facility	11-48
Copy Error Log or Trace Log to Transfer Directory	11-53
Export Problem Determination Output	11-53
Using the IBM 6611 Performance and Statistics Facilities	11-54
View Protocol and Interface Packet Traffic Information	11-55
View Network Management Information	11-57
View System Activity Report	11-59
View Process Information and Status	11-61
View Adapter Interface Statistics	11-69
View System Network Statistics	11-75
View Virtual Memory Statistics	11-87
View Input/Output Statistics	11-88
Export Performance Data	11-89
Chapter 12. Using the Software Installation and Maintenance Facility	12-1
About This Chapter	12-2
Software Component and Update Packaging	12-2
Installing Software Changes	12-3
Installing Software Updates	12-3
Installing Software Components	12-5
Restarting System after Software Installation	12-6
Software Installation Procedure	12-6
Post Software Installation Functions	12-16
Automating Software Installation and Maintenance Facility Functions	12-19
Sending Software Updates to One IBM 6611	12-19
Sending Software Updates to Multiple IBM 6611s	12-21
Sending Software Components to Multiple IBM 6611s	12-23
Transferring Software Changes to an IBM 6611	12-25
Transferring Software from a Diskette to an IBM 6611	12-26
Transferring Software from Diskette to the RISC System/6000 Workstation	12-27
Transferring Software from a RISC System/6000 Workstation to an IBM 6611 Using FTP	12-28
Transferring Software from an IBM 6611 to an IBM 6611 Using FTP	12-30
Transferring Software from a RISC System/6000 Workstation to an IBM 6611 Using Xmodem	12-32
Saving Your Software and Configuration Diskettes	12-33
Software Vital Product Data	12-33

List All Installed Software	12-35
List All Updates to a Software Component	12-35
List Files Included in a Software Component	12-36
List Prerequisites of a Software Component	12-36
List Dependents of a Software Component	12-37
View ID of a Software Component	12-38
View History of a Software Component	12-38
Verify a Software Component	12-39
Exporting the Software Vital Product Data	12-40
 Chapter 13. Using Concurrent Diagnostics and Hardware Vital Product Data	13-1
Running Concurrent Hardware Diagnostics	13-2
From a Direct-Attached ASCII Terminal	13-2
From a Modem-Attached ASCII Terminal	13-5
From a Workstation on the IP Network	13-5
Hardware VPD Format	13-6
Viewing Hardware Component Information	13-7
Viewing Hardware Vital Product Data	13-12
Updating the Hardware VPD after Configuration Changes	13-12
 Chapter 14. Using the System Manager to Configure the IBM 6611	14-1
About This Chapter	14-4
Updating Configuration Parameters	14-4
Configuration Objects	14-7
Configuration Procedure	14-8
Initial Configuration Using a Diskette	14-11
Initial Configuration without Using a Diskette	14-11
Direct IP Attachment	14-12
Modem Transfer Method	14-12
FTP Transfer Method	14-14
Minimal Configuration Using the System Manager	14-15
Importing and Exporting the Configuration File	14-17
Reinstating a Saved Configuration File	14-19
Working with the Configuration Information Text Files	14-20
Configuration Report	14-20
Configuration Error Message Report	14-22
Configuration Script	14-23
Export Configuration Information	14-25
Box-Level Single Objects	14-26
Parameters for AppleTalk	14-26
APPN Parameters	14-26
APPN Thresholds	14-26
Parameters for BGP	14-26
Protocol Bridging Parameters	14-27
Bridging Spanning Tree Parameters	14-27
Configuration Process Parameters	14-27
DECnet Parameters	14-27
Data Link Switching Parameters	14-28
Parameters for EGP	14-28
Hello Parameters	14-28
IP Parameters	14-28
IPX Parameters	14-29
Software Lock Parameters	14-29
NetBIOS Filter Parameters	14-29
OSPF Parameters	14-29
Protocol – Independent Parameters	14-29

RIP Parameters	14-30
SNA Frame Filter Parameters	14-30
SNMP System Contact	14-30
SNMP System Name	14-30
SNMP System Location	14-30
SNMP Parameters	14-31
Serial Line TTY Parameters	14-31
XNS Parameters	14-31
Transparent Bridging Parameters	14-31
Transparent Bridging Spanning Tree Parameters	14-32
Transparent Bridging Destination Values	14-32
XNS Static Route Tables Parameters	14-32
APPN Parameters for Threshold (Accessed from System Manager-ONLY)	14-33
Port-Level Single Objects	14-34
AppleTalk DLCI Available on a Port	14-34
AppleTalk Port Values	14-34
Source Route Bridging Parameters	14-35
DECnet Parameters	14-36
Ethernet Adapter Parameters	14-36
IP Parameters	14-36
IP Filter Parameters	14-36
IPX Parameters	14-37
SDLC Adapter Parameters	14-37
Transparent Bridging Port Parameters	14-38
NetBIOS Packet Forwarding Parameters	14-39
EIA 422/449 Serial Adapter or V.35/V.36 Serial Adapter Port Parameters	14-39
IBM LAN Bridge Parameters	14-39
Frame Relay Parameters	14-40
Point-to-Point Protocol Parameters	14-40
SNA Parameters	14-40
Token-Ring Adapter Parameters	14-40
X.25 Parameters	14-40
X.25 Subscription Parameters	14-41
X.25 Network Tuning Parameters	14-41
X.25 Subscription PVC Default Parameters	14-42
X.25 Subscription SVC Parameters	14-42
XNS Parameters	14-43
Port-Level List Objects	14-43
List of AppleTalk Packet Filters	14-43
List of Additional AppleTalk Zone Names	14-43
List of MAC Input Filters for SRB	14-43
List of Ring Input Filters for SRB	14-44
List of SAP Input Filters for SRB	14-44
List of SNAP Input Filters for SRB	14-44
List of MAC Output Filters for SRB	14-44
List of Ring Output Filters for SRB	14-44
List of SAP Output Filters for SRB	14-44
List of SNAP Output Filters for SRB	14-44
List of Ring Number—DLCI Pairs for SRB	14-44
List of MAC Input Filters for TB	14-45
List of SAP Input Filters for TB	14-45
List of Sliding Window Input Filters for TB	14-45
List of SNAP Input Filters for TB	14-45
List of Logical Ports Number to DLCI Pairs for TB	14-45
List of MAC Output Filters for TB	14-45
List of SAP Output Filters for TB	14-45

List of Sliding Window Output Filters for TB	14-46
List of SNAP Output Filters for TB	14-46
List of DECnet Node to DLCI Mappings	14-46
List of DECnet Packet Filters	14-46
List of Multicast MAC Addresses	14-46
List of IP Destination Address to DLCI Mappings	14-46
List of IP Parameters for X.25	14-47
List of IPX Destination Address to DLCI Mappings	14-47
List of IPX Filters	14-48
List of SNA Stations for Adapter	14-49
List of DLCIs Attached to Frame Relay	14-49
List of SAP Values	14-49
List of X.25 Subscription PVC Parameters	14-49
List of XNS Destination Address to DLCI Mappings	14-50
List of XNS Filters	14-50
Box Level List Objects	14-50
List of Valid Configuration Hosts	14-50
List of DECnet Packet Filters	14-51
List of Participating DLS Routers	14-51
List of GATED Export Parameters	14-51
List of No-HELLO-In/No-HELLO-Out Settings	14-51
List of Hello Source Routers	14-51
List of Hello Trusted Routers	14-52
List of IP Packet Filters	14-52
List of IP Static Routes	14-52
List of Inbound IPX RIP Filter Parameters	14-52
List of Outbound IPX RIP Filter Parameters	14-52
List of IPX Router Filters	14-53
List of IPX SAP Filters	14-53
List of NetBIOS Default Destinations	14-53
List of NetBIOS Destination Name Filters	14-53
List of NetBIOS Source Name Filters	14-53
List of Static Host to Internet Address Mappings	14-53
List of No-RIP-In/No-RIP-Out Settings	14-54
List of RIP Source Routers	14-54
List of RIP Trusted Routers	14-54
List of Remote Name Servers	14-54
List of Remote Time Servers	14-54
List of SNA Default Destinations	14-54
List of SNA Destination Frame Filters	14-54
List of SNA Source Frame Filters	14-55
List of SNMP Clients for Traps	14-55
List of SNMP Communities	14-55
List of Controlling User Names and Passwords	14-55
List of Viewing User Names and Passwords	14-56
List of XNS RIP Inbound Filters	14-56
List of XNS RIP Outbound Filters	14-56
List of XNS RIP Router Filters	14-56
List of Transparent Bridging Filters	14-56
Appendix A. Configuration Planning Worksheets	A-1
Appendix B. Error and Status Codes	B-1
Appendix C. License Program Specification	C-1
Description	C-1

Specified Operating Environment	C-1
Machine Requirements	C-1
Programming Requirements	C-2
Licensed Program Materials Availability	C-2
Supplemental Terms	C-3
Testing Period	C-3
Installation/Location License	C-3
Usage License	C-3
Type/Duration of Program Services	C-3
Warranty	C-3
Additional Information	C-3
 List of Abbreviations and Acronyms	 X-1
 Glossary	 X-3
 Index	 X-25

Figures

1-1.	Sample Network for Getting Started	1-3
1-2.	Sample Planning Chart	1-4
1-3.	Sample Configuration Worksheet	1-5
1-4.	Sample Configuration Worksheet	1-6
1-5.	Sample Configuration Worksheet	1-6
1-6.	Sample Configuration Worksheet	1-7
1-7.	Sample Configuration Worksheet	1-7
1-8.	Sample Configuration Worksheet	1-8
1-9.	Sample Configuration Worksheet	1-8
1-10.	Sample Configuration Worksheet	1-9
2-1.	Configuration Program Installation Screen	2-5
2-2.	Configuration Program Logo Screen	2-7
2-3.	Main Window of the Configuration Program	2-8
2-4.	System Configuration Window	2-10
2-5.	System Management Window	2-11
2-6.	Port Summary Window	2-11
2-7.	Port-Level Parameters Window	2-12
3-1.	Sample Network Using Data Link Switching	3-20
5-1.	SDLC Adapter Ports	5-21
7-1.	System Manager Main Menu	7-4
7-2.	System Configuration Information Screen	7-6
7-3.	Example of a Selector Screen	7-6
7-4.	Example of a Dialog Screen	7-7
7-5.	Example of a Command Status Screen	7-9
7-6.	System Manager Main Menu	7-14
7-7.	System Manager Help	7-15
7-8.	System Manager Main Menu	7-16
7-9.	System Manager Menu Tree Part I	7-18
7-10.	System Manager Menu Tree Part II	7-20
7-11.	Performance and Statistics Menu	7-22
7-12.	Problem Determination Facilities Menu	7-23
7-13.	Diagnostic Operating Instructions Screen	7-26
7-14.	Function Selection Menu	7-26
7-15.	Resource Control and Management Menu	7-27
7-16.	System Environment and Configuration Menu	7-28
7-17.	Remote Accesses to Other Nodes	7-30
7-18.	Software Installation and Maintenance Menu	7-31
7-19.	View Software Vital Product Data Menu	7-32
7-20.	Hardware Vital Product Data Menu	7-34
7-21.	Configuration Files and Reports Menu	7-35
7-22.	Adapter and Protocol Configuration Screen 1	7-37
7-23.	Adapter and Protocol Configuration Screen 2	7-37
9-1.	IBM 6611 with No Attachments	9-2
9-2.	Direct-Attached Terminal	9-3
9-3.	Network-Attached Terminal	9-4
9-4.	Modem-Attached Terminal	9-5
9-5.	Extended Network Configuration	9-5
9-6.	Remote Accesses to Other Nodes Menu	9-8
9-7.	General Setup Attributes for the IBM 3101 ASCII Terminal	9-19
10-1.	Resource Control and Management Menu	10-3
10-2.	Sample Output from Reading the 3-Digit Display	10-7
10-3.	View System Route Table Example	10-9

10-4.	Adapter Route Table Example	10-10
10-5.	Example of View Network Management Subsystem Information Output	10-12
10-6.	Manage ARP Tables Menu Screen	10-13
10-7.	Example of Export Route Information to UNIX Diskette	10-18
10-8.	System Environment and Configuration Screen	10-19
10-9.	Viewing a Transfer Directory File	10-20
10-10.	Viewing a Static Directory File	10-21
10-11.	Performing Diskette Operations Menu	10-23
10-12.	System Configuration Information Screen	10-29
10-13.	Perform System Configuration Changes Menu	10-30
10-14.	Configure Userids and Passwords Menu	10-32
10-15.	Configure Host Name to IP Address Mapping Menu	10-35
10-16.	Configure Remote Host Name Service Menu	10-37
10-17.	Configure Remote Time Service Menu	10-39
10-18.	Pop-Up Screen Used to Direct Output	10-45
10-19.	Remote Accesses to Other Nodes	10-54
11-1.	Problem Determination Facilities Menu	11-4
11-2.	Example of a Summary Error Report	11-7
11-3.	Example of View an Error Report for a Single Sequence Number for a Software Error	11-8
11-4.	Example of View an Error Report for a Single Sequence Number for a Hardware Error	11-9
11-5.	Use System and User Process Dump Facilities Menu	11-11
11-6.	Example of View Previous System Dump Information Output	11-13
11-7.	Example of Copy System Dump to Diskette or Transfer Directory Status Message	11-14
11-8.	Example of View a Formatted System Dump Output	11-15
11-9.	Example of Start User Process Memory Dump Status Output	11-17
11-10.	Example of View User Process Memory Dump Output	11-18
11-11.	Example of Start IP Routing Protocols Dump Status Messages	11-19
11-12.	Example of View IP Routing Protocols Dump Output	11-20
11-13.	Use System Trace Facility Menu	11-21
11-14.	Example of View System Trace Report Output	11-23
11-15.	Use Special User Process Traces Menu	11-24
11-16.	Use IP Routing Protocols Trace Menu	11-25
11-17.	Example of View IP Routing Protocols Trace Output	11-27
11-18.	Example of Start and Stop SNMP Trace Output	11-28
11-19.	Example of View SNMP Trace Output	11-29
11-20.	Example of System Monitor Trace Log	11-30
11-21.	Example of X.25 Trace Output	11-30
11-22.	Use AppleTalk Trace Menu	11-31
11-23.	Example of View AppleTalk Protocol Trace Output	11-33
11-24.	Use APPN Trace Menu	11-34
11-25.	Example of View APPN Trace Report Output	11-36
11-26.	Use Adapter Debug Facility Menu	11-37
11-27.	Example of Read Adapter Memory Output	11-39
11-28.	Example of View Adapter Registers Output	11-39
11-29.	Sample Adapter Line Trace Output - Record 1	11-40
11-30.	Example of Start Adapter Line Trace Message	11-41
11-31.	Example of Dump Adapter Memory Message	11-41
11-32.	Example of View Adapter Debug Data in Transfer Directory Output	11-42
11-33.	Use Source Route Bridging Debug Facility Menu	11-43
11-34.	Example of Use Source Route Bridging Debug Facility Output	11-44
11-35.	Example of Start Bridging Frame Trace Message	11-45
11-36.	Example of Stop Bridging Frame Trace Message	11-45

11-37.	Example of View Bridging Frame Trace Output	11-46
11-38.	Example of View Bridge Configuration Information Message	11-47
11-39.	Example of View Bridge SAP Filter Information Output	11-47
11-40.	Use DECnet Debug Facility Menu	11-48
11-41.	Example of Circuit Vector Entry	11-50
11-42.	Example of Executor Data Structure	11-50
11-43.	Example of DECnet Trace Output	11-52
11-44.	Example of Copy Error Log or Trace Log to Transfer Directory Output	11-53
11-45.	Example of Export Problem Determination Output Using Modem	11-54
11-46.	Performance and Statistics Menu	11-55
11-47.	Sample View Protocol and Interface Packet Traffic Information Panel	11-56
11-48.	Example of View Network Management Information Output	11-59
11-49.	Example of View System Activity Report Output	11-60
11-50.	View Process Information and Status Menu	11-61
11-51.	Example of List Processes Output	11-62
11-52.	Example of List Process Commands output	11-63
11-53.	Example of View Process Information Output	11-65
11-54.	Example of View Process Status Output	11-67
11-55.	Example of View Process Table Information Output	11-68
11-56.	View Adapter Interface Statistics Menu	11-69
11-57.	Example of Connection Statistics Output	11-70
11-58.	Example of Protocol Statistics Output	11-72
11-59.	Example of Packet Traffic Statistics Output	11-73
11-60.	Example of Filter Information Output for DECnet	11-74
11-61.	Example of Bridge Statistics Output	11-74
11-62.	Example of LAN Bridge Statistics Output	11-75
11-63.	View System Network Statistics Menu	11-76
11-64.	Example of Connection Statistics Output	11-77
11-65.	Example of TCP/IP Protocol Statistics Output	11-78
11-66.	Example of Packet Traffic Statistics Output	11-80
11-67.	Example of Memory Management Statistics Output	11-80
11-68.	Example of TCP/IP Route Statistics Output	11-81
11-69.	Example of System Socket Information Output	11-81
11-70.	Example of Active Internet Connection Information Output	11-82
11-71.	Example of Source Route Bridge Spanning Tree Statistics Output	11-82
11-72.	Example of Source Route Bridge Spanning Tree Frame Relay Statistics Output	11-83
11-73.	Example of Transparent Bridge Spanning Tree Statistics Output	11-84
11-74.	Example of Transparent Bridge Spanning Tree Frame Relay Statistics Output	11-85
11-75.	Example of LAN Bridge Statistics Output	11-86
11-76.	Example of LAN Bridge Internal Protocol Frame Statistics Output	11-87
11-77.	Example of View Virtual Memory Statistics Output	11-88
11-78.	Example of View Input/Output Statistics Output	11-88
11-79.	Example of Export Performance Data to DOS Diskette	11-89
12-1.	Software Installation and Maintenance Menu	12-7
12-2.	Sample List of Software in Transfer Directory	12-8
12-3.	Sample List of Problems Fixed by Software Updates	12-9
12-4.	Software Update Installation Output	12-11
12-5.	Software Component Installation Output	12-13
12-6.	System Restart Messages	12-14
12-7.	List of Applied But Not Committed Software Example	12-17
12-8.	A Sample Script That Applies All Software Updates	12-20
12-9.	A Sample Configuration for Installing Software	12-21
12-10.	Example apply_updt.in Input File	12-22

12-11.	Example of the apply_updt.out File	12-23
12-12.	Example apply_comp.in Input File	12-24
12-13.	Example of the apply_comp.out File	12-25
12-14.	Example of the apply_comp_out File	12-25
12-15.	View Software Vital Product Data Menu	12-34
12-16.	Sample List of All Installed Software	12-35
12-17.	Sample List of All Updates to Software Components	12-35
12-18.	Sample List of Files for Software Components	12-36
12-19.	Sample List of Prerequisites for Software Components	12-37
12-20.	Sample List of Dependents for Software Components	12-37
12-21.	Sample List of Files for Software Components	12-38
12-22.	Sample List of History Information for Software Components	12-39
12-23.	Software Verification Output Example	12-39
12-24.	Example of Export Software Vital Product Data to DOS Diskette	12-40
13-1.	First Screen of Diagnostics Programs	13-2
13-2.	FUNCTION SELECTION Screen	13-3
13-3.	Diagnostic Mode Selection Screen	13-4
13-4.	Example of Diagnostic Selection Screen in the Diagnostics Program	13-4
13-5.	Hardware Vital Product Data Menu	13-8
13-6.	Listing Supported Devices Output	13-9
13-7.	Example List of Defined Devices	13-10
13-8.	List of Installed Devices Example	13-11
13-9.	View Characteristics of a Defined Device Example	13-11
13-10.	Viewing Hardware VPD Example	13-12
13-11.	Update Hardware VPD after Configuration Changes Example Output	13-13
13-12.	Example of Export Hardware Vital Product Data Output Using FTP	13-14
14-1.	System Configuration Information Screen	14-6
14-2.	Warning Screen for the Adapter and Protocol Configuration Menu Item	14-7
14-3.	Menu Screen for the Adapter and Protocol Configuration Main Menu Item	14-8
14-4.	Select Parameter Level Selector Screen	14-9
14-5.	Sample Adapter Slot Number Selector Screen	14-9
14-6.	Sample Adapter Port Number Selector Screen	14-10
14-7.	Configuration Files and Reports Menu	14-13
14-8.	Import Method Selector Screen	14-18
14-9.	Export Method Selector Screen	14-19
14-10.	Detailed Configuration Report Example	14-21
14-11.	Brief Configuration Report Example	14-22
14-12.	Sample Configuration Error Message Report	14-23
14-13.	Sample Configuration Script	14-24
14-14.	Sample RSH Configuration Script	14-24
14-15.	Example of Export Configuration Information Output Using FTP	14-25

Tables

0-1.	IBM 6611 Adapter Names	xxvi
0-2.	IBM 6611 and Multiprotocol Network Program Libraries	xxvii
1-1.	Configuration Parameters That Restart a Function — SRB	1-12
1-2.	Configuration Parameters That Restart a Function — DLS	1-12
1-3.	Configuration Parameters That Restart a Function — SNA	1-13
1-4.	Configuration Parameters That Restart a Function — SNA	1-13
1-5.	Configuration Parameters That Restart a Function — NetBIOS	1-13
1-6.	Configuration Parameters That Restart a Function — BGP	1-13
1-7.	Configuration Parameters That Restart a Function — EGP	1-14
1-8.	Configuration Parameters That Restart a Function — Hello	1-15
1-9.	Configuration Parameters That Restart a Function — IP	1-15
1-10.	Configuration Parameters That Restart a Function — IPX	1-15
1-11.	Configuration Parameters That Restart a Function — NetBIOS	1-15
1-12.	Configuration Parameters That Restart a Function — OSPF	1-15
1-13.	Configuration Parameters That Restart a Function — RIP Import	1-16
1-14.	Configuration Parameters That Restart a Function — RIP	1-16
1-15.	Configuration Parameters That Restart a Function — LAN Bridge	1-16
1-16.	Configuration Parameters That Restart a Function — SRB Ports	1-17
1-17.	Configuration Parameters That Restart a Function — IP/X.25	1-17
1-18.	Configuration Parameters That Restart a Function — SDLC	1-18
1-19.	Configuration Parameters That Restart a Function — SNA Ports	1-18
1-20.	Configuration Parameters That Restart a Function — X.25 Ports	1-18
1-21.	Configuration Parameters That Restart a Function — SNA Stations	1-19
1-22.	Configuration Parameters That Restart a Function — APPN Parameters	1-19
1-23.	Configuration Parameters That Restart AppleTalk on Affected Port-Only (Valid for Ethernet and Token-Ring Ports)	1-20
1-24.	Configuration Parameters That Restart the IBM 6611 — DECnet	1-21
1-25.	Configuration Parameters That Restart the IBM 6611 — DECnet Ports	1-21
1-26.	Configuration Parameters That Restart the IBM 6611 — Ethernet Adapter	1-21
1-27.	Configuration Parameters That Restart the IBM 6611 — Frame Relay	1-21
1-28.	Configuration Parameters That Restart the IBM 6611 — PPP	1-21
1-29.	Configuration Parameters That Restart the IBM 6611 — serial adapter	1-22
1-30.	Configuration Parameters That Restart the IBM 6611 — Token-Ring Network 16/4 Adapter	1-22
1-31.	Configuration Parameters That Restart the IBM 6611 — Transparent Bridging	1-22
1-32.	Configuration Changes That Restart the IBM 6611 — AppleTalk	1-22
2-1.	MPNP Configuration Program Menu Bar	2-9
3-1.	SNA and NetBIOS Configuration Requirements	3-18
3-2.	APPN Configuration Options	3-33
6-1.	IBM 6611 Adapters and Supported Protocols	6-4
6-2.	Valid Values and Default Values for Maximum Transmission Unit	6-52
6-3.	AppleTalk Configuration Options	6-59
7-1.	System Manager Function Keys	7-11
7-2.	Performance and Statistics Table	7-23
7-3.	Problem Determination Facilities Table	7-25
7-4.	Resource Control and Management Table	7-28
7-5.	System Environment Table	7-29
7-6.	Remote Accesses to Other Nodes Table	7-31
7-7.	Software Installation and Maintenance Table	7-33

7-8.	Hardware VPD	7-35
7-9.	System Configuration Management Table	7-36
8-1.	Group Prefixes for Accessing Help in the Fast-Path Environment	8-8
9-1.	General Setup Attributes for the ASCII Terminal or Emulator	9-20
9-2.	Communication Setup Attributes for the ASCII Terminal or Emulator	9-21
10-1.	Adapter Interface Name Table	10-8
10-2.	Output File Names Generated from Performance and Statistics Menu Items	10-46
10-3.	Output File Names Generated from Problem Determination Facilities Menu Items	10-47
10-4.	Output File Names Generated from Resource Control and Management Menu Items	10-48
10-5.	Output File Names Generated from Software Installation and Maintenance Menu Items	10-49
10-6.	Output File Names Generated from Hardware Vital Product Data Menu Items	10-49
10-7.	Output File Names Generated from Configuration Files and Reports Menu Items	10-49
10-8.	Output File Names not Generated from System Manager	10-50
10-9.	Output File Names for Pruned Files	10-50
10-10.	Output File Names for Removed Files	10-50
11-1.	Adapter Name Table	11-37
11-2.	Adapter Interface Name Table	11-43
11-3.	Interface Name Table	11-57
11-4.	Adapter Interface Name Table	11-69
11-5.	Adapter Interface Name Table	11-76

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to: IBM Director of Commercial Relations, IBM Corporation, Purchase, NY 10577, U.S.A.. The licensed program described in this document and all licensed material for it are provided by IBM under terms of the IBM Customer Agreement.

This document is not intended for production use and is furnished as is without any warranty of any kind, and all warranties are hereby disclaimed including the warranties of merchantability and fitness for a particular purpose.

Trademarks

The following terms, denoted by an asterisk (*) in this publication, are trademarks or registered trademarks of the IBM Corporation in the United States or other countries:

Advanced Peer-to-Peer Networking	APPN
AIX	AIXwindows
IBM	NetView
Personal System/2	PS/2
RISC System/6000	SAA
Systems Application Architecture	

The following terms, denoted by a double asterisk (**) in this publication, are trademarks of other companies:

AppleTalk	Apple Computer, Inc.
Cisco	Cisco Systems, Inc.
Cylink	Cylink Corporation
DECnet	Digital Equipment Corporation
Digital	Digital Equipment Corporation
Intel	Intel Corporation
Internetwork Packet Exchange	Novell Corporation
IPX	Novell Corporation
Microsoft Windows	Microsoft Corporation
MS-DOS	Microsoft Corporation
NetWare	Novell, Inc.
Novell	Novell, Inc.
OSF/Motif	Open Software Foundation, Inc.
Xerox	Xerox Corporation
Xerox Network Systems	Xerox Corporation
XNS	Xerox Corporation

UNIX
80386

Unix System Laboratories, Inc.
Intel Corporation

About This Book

This book describes how to use the IBM Multiprotocol Network Program Version 1 Release 1.1 and Version 1 Release 1.2. The Multiprotocol Network Program (5648-016) is the operating system that provides the bridging and routing functions for the IBM 6611 Network Processor (*IBM 6611*). The Multiprotocol Network Program is preloaded on the disk of the IBM 6611. There are three components of the Multiprotocol Network Program:

- The base operating system performs routing and bridging and supports the Simple Network Management Protocol (SNMP) network manager agent.
- The IBM Multiprotocol Network Program Configuration Program (*Configuration Program*) allows you to customize the IBM 6611 functions and communication with the network. The Configuration Program diskettes may have been shipped separately for the IBM 6611. You should store the diskettes in the diskette holders and store them along with this book inside the binder.
- The IBM Multiprotocol Network Program System Manager (*System Manager*) is a user interface that performs operation and system management tasks.

This book consists of:

- “Part I: Using the Configuration Program”

Chapter 1 explains how to configure the IBM 6611.

Chapter 2 explains how to install and operate the Configuration Program, and how to transport the configuration file.

Chapter 3 provides details about each configuration parameter that relates to the system setup.

Chapter 4 provides details about each configuration parameter that relates to system management.

Chapter 5 provides details about each configuration parameter that relates to the adapters that are installed.

Chapter 6 provides details about each configuration parameter that relates to the protocols you are using.

- “Part II: Using the System Manager”

Chapter 7 explains how to use the System Manager and the tasks that can be performed using the System Manager.

Chapter 8 describes the command primitives used in the fast path environment, or with **rsh** and **rexec** commands.

Chapter 9 explains how to access the IBM 6611 locally and remotely and describes the access commands that are supported by the IBM 6611.

Chapter 10 explains how to perform operations using the System Manager.

Chapter 11 provides procedures for identifying and reporting problems. It also includes instructions for obtaining traces, dumps, and performance data that you may need to generate for the IBM service personnel.

Chapter 12 explains how to install software updates to the IBM 6611. It also contains information about software vital product data.

Chapter 13 provides information about hardware vital product data and concurrent hardware diagnostics.

Chapter 14 explains how to use the System Manager to perform configuration.

- **Appendixes**

Appendix A provides worksheets to be filled in with the configuration parameters of the IBM 6611.

Appendix B lists error and status codes that are displayed by the IBM 6611 during initialization and operation. A user response is included for each code.

Appendix C provides license information for the IBM Multiprotocol Network Program.

- A list of abbreviations, a glossary, and an index follow the appendixes.

Summary of Changes

This is the third edition of the *IBM Multiprotocol Network Program User's Guide*. Since the second edition was published, support for the Model 120 has been added to the IBM Multiprotocol Network Program.

The Model 120 is available in eight fixed configurations, which differ according to the combination of adapters installed. Some of the adapters supported by the Model 120 are identical to those supported by the Model 140 and Model 170; others are physically distinct from but functionally equivalent to the adapters supported by the Model 140 and Model 170.

For the sake of brevity, we will refer to equivalent adapters by one generic name. Table 0-1 lists the adapters supported by each model of the IBM 6611 and the generic name used in this publication.

Table 0-1. IBM 6611 Adapter Names		
Model 140 and Model 170	Model 120	Generic
6611 Token-Ring Network 16/4 Adapter	6611 Model 120 Token-Ring Network 16/4 Adapter	Token-Ring Network 16/4 Adapter
6611 Ethernet Adapter	6611 Model 120 Ethernet Adapter	Ethernet Adapter
6611 2-Port EIA 422/449 Serial Adapter	6611 Model 120 2-Port EIA 422/449 Serial Adapter	EIA 422/449 Serial Adapter
6611 2-Port V.35/V.36 Compatible Serial Adapter	6611 Model 120 2-Port V.35/V.36 Compatible Serial Adapter	V.35/V.36 Serial Adapter
6611 X.25 Adapter	6611 X.25 Adapter	X.25 Adapter
6611 4-Port SDLC Adapter	6611 4-Port SDLC Adapter	SDLC Adapter

This edition contains information about the new adapters as well as miscellaneous corrections and clarifications of information in the second edition.

Who Should Use This Book

This book is intended for the customer who will configure and manage the IBM 6611. The users include the network planner, system programmer, network administrator, and network operator.

IBM 6611 and Multiprotocol Network Program Libraries

Table 0-2 indicates the primary tasks supported by each book in the IBM 6611 and Multiprotocol Network Program libraries.

Table 0-2. IBM 6611 and Multiprotocol Network Program Libraries

Model	Planning and Ordering	Installing	Configuring	Operating	Problem Solving	Servicing
120	1, 9	4, 7	5, 8, 9	4, 5	2, 4, 5, 6	2, 3, 5, 6
140/170	1, 9	2, 3	5, 8, 9	4, 5	2, 4, 5, 6	2, 3, 5, 6

Legend:

- 1 IBM 6611 Network Processor Introduction and Planning Guide, GK2T-0334
- 2 IBM 6611 Network Processor Installation and Service Guide, GA27-3941
- 3 IBM 6611 Network Processor Translated Safety Information, GA27-3954
- 4 IBM 6611 Network Processor Operations Pocket Guide, GX27-3909
- 5 IBM Multiprotocol Network Program User's Guide, SC30-3559
- 6 IBM 6611 Network Processor Network Management Reference, GC30-3567
- 7 IBM 6611 Network Processor Model 120 Customer Setup Guide, GA27-3993
- 8 IBM Multiprotocol Network Program Configuration Quick Reference, GX27-3927
- 9 IBM Multiprotocol Network Program Implementation of the DECnet Phase IV-Prime Protocol, SD21-0054

The publications numbered 2, 3, and 4 are shipped with all models of the IBM 6611. Publication 7 is shipped with the Model 120. All of the publications may be ordered from IBM using the form numbers shown. Contact an IBM representative for assistance in ordering a publication.

Part I: Using the Configuration Program

The chapters in “Part I: Using the Configuration Program” are:

Chapter 1. Preparing for Configuration	1-1
Chapter 2. Using the Configuration Program	2-1
Chapter 3. System Configuration Parameters	3-1
Chapter 4. System Management Parameters	4-1
Chapter 5. Adapter Configuration Parameters	5-1
Chapter 6. Protocol Configuration Parameters	6-1

Chapter 1. Preparing for Configuration

About this Chapter	1-2
Getting Started	1-3
Configuration Considerations	1-10
General Recommendations for Configuration	1-10
Planning for Network Implementation	1-10
Setting Up a Network for Simulation	1-10
Implementing a Limited Production Network	1-10
Implementing Your Full Production Network	1-11
Configuration Trouble Shooting	1-11
Changing Configuration Parameters	1-11
Fully Dynamic Configuration Changes	1-11
Configuration Changes Requiring the Function to Restart	1-12
Configuration Changes Requiring the IBM 6611 to Restart	1-20

About this Chapter

This chapter explains how to prepare to configure an IBM 6611. See Chapter 3 through Chapter 6 for explanations about the configuration parameters. The information in Chapter 3 through Chapter 6 is arranged in the same order as the worksheets in Appendix A, so that you can reference them easily. Two programs allow you to configure the IBM 6611 Network Processor (*IBM 6611*):

1. IBM Multiprotocol Network Program Configuration Program (*Configuration Program*).

The Configuration Program offers a graphical user interface that allows you to configure the IBM 6611 from a stand-alone workstation. The Configuration Program interface is based on OSF/Motif**. The Configuration Program must be operated from an IBM RISC System/6000* workstation or IBM Personal System/2* (PS/2*) workstation. On a RISC System/6000 workstation, the configuration file can be sent to the IBM 6611 after using the Configuration Program. The Configuration Program provides:

- Error checking for valid parameter values
- Ability to perform dependency checking on related parameters
- Ability to retain configuration information that can be used in subsequent configurations or reconfigurations
- On line help
- User-friendly, graphical interface.

These characteristics recommend the Configuration Program as the preferred way to perform configuration. See Chapter 2 for more information about using the Configuration Program.

2. IBM Multiprotocol Network Program System Manager (*System Manager*).

The System Manager is a menu-driven, interactive user interface that is designed to perform change management, network management, problem determination, and configuration. It can be accessed locally or remotely by attaching an ASCII terminal to the IBM 6611 or by issuing a remote network access command: for example, the **telnet** command can be used to access the IBM 6611. The System Manager configuration is accessed by selecting **Adapter and Protocol Configuration** from the main menu.

The System Manager provides:

- The ability to perform minimal configuration to attach the IBM 6611 to the network.
- A user interface to change configuration parameters while directly attached to the IBM 6611. However, the System Manager configuration facility provides minimal error checking, which includes no dependency checking on related parameters.

See Chapter 14 for more information about using the System Manager to perform configuration.

Before you start to fill out the IBM 6611 Network Processor Configuration Worksheets (*Configuration Worksheets*), you need one of the Planning Charts from the *IBM 6611 Network Processor Introduction and Planning Guide* and the *About Your Machine* sheet that is provided with the IBM 6611. A Planning Chart lists which protocols and functions are available for you to configure in the IBM 6611. The *About Your Machine* sheet lists which adapter is placed in each slot.

Make copies of the worksheets needed to perform system level configuration, which includes System Configuration and System Management parameters.

Determine the worksheets you need to fill out for the adapters. Make copies of the worksheets for each adapter in your machine.

Note: It is very important that you complete the preliminary information at the top of each worksheet. This information is specific to each IBM 6611, and it will help you keep the configuration information in order.

After completing the adapter worksheets, select the worksheets for the protocols that will be used on each port. For each of the protocols being used, make a copy of the worksheet.

The order of the worksheets in Appendix A is the recommended sequence for configuring the IBM 6611. On the worksheets, required parameters are denoted by an (R), and default values are represented by a (†) dagger.

Getting Started

This section explains how to configure the IBM 6611. A sample scenario is provided to explain step-by-step instructions to prepare the configuration worksheet before using the Configuration Program.

Figure 1-1 shows the sample network that is being configured.

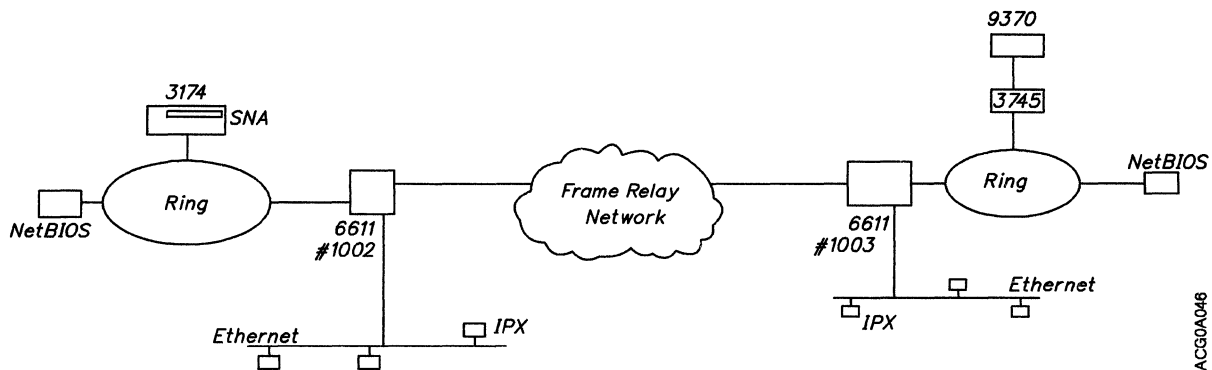


Figure 1-1. Sample Network for Getting Started

The IBM 6611 Network Processor Planning Charts can be found in the IBM 6611 Network Processor Introduction and Planning Guide. The system administrator completes a planning chart to record which adapters and protocols will be used in the IBM 6611. The planning chart can be used as a reference when the system administrator prepares the IBM 6611 Configuration Worksheets. Figure 1-2 on page 1-4 shows a sample planning chart for the Model 140 that contains the adapters and protocols which are used in Figure 1-1.

IBM 6611 Network Processor Planning Chart for the Models 140 and 170

Completed by J. Doe Date 6/26/92

Fill out one chart for each IBM 6611 Network Processor.

Unit Number or Name 1002 Model Type: ☒ Model 140 ☐ Model 170
 Location: Building/Floor CHQ/205
 Site Capital City

Slot	Adapter	Port	Protocols	Functions		
1	Adapter Type	Port Number	Protocol Name	Routing	Bridging	Data Link Switching
		<u> </u>	<u> </u>	☐	☐	☐
		<u> </u>	<u> </u>	☐	☐	☐
		<u> </u>	<u> </u>	☐	☐	☐
		<u> </u>	<u> </u>	☐	☐	☐
2	Adapter Type	Port Number	Protocol Name	Routing	Bridging	Data Link Switching
	EIA 422/449 Serial	<u>1</u>	<u>IPX</u>	☒	☐	☐
		<u>1</u>	<u>Frame Relay</u>	☐ N/A	☐ N/A	☐ N/A
		<u>1</u>	<u>SNA, NetBIOS</u>	☐	☒	☐
		<u> </u>	<u> </u>	☐	☐	☐
3	Adapter Type	Port Number	Protocol Name	Routing	Bridging	Data Link Switching
	Ethernet	<u>1</u>	<u>IPX</u>	☒	☐	☐
		<u> </u>	<u> </u>	☐	☐	☐
		<u> </u>	<u> </u>	☐	☐	☐
		<u> </u>	<u> </u>	☐	☐	☐
4	Adapter Type	Port Number	Protocol Name	Routing	Bridging	Data Link Switching
	Token- Ring	<u>1</u>	<u>SNA, NetBIOS</u>	☐	☒	☐
		<u> </u>	<u> </u>	☐	☐	☐
		<u> </u>	<u> </u>	☐	☐	☐
		<u> </u>	<u> </u>	☐	☐	☐

* Maximum 4 adapters in Model 140; maximum 7 adapters in Model 170.

Adapter	Feature Code	Adapter Type
6611 2-Port EIA 422/449 Serial Adapter	2640	EIA 422/449 Serial
6611 2-Port V.35/V.36 Compatible Serial Adapter	2650	V.35/V.36 Serial
6611 Token-Ring Network 16/4 Adapter	2660	Token-Ring
6611 Ethernet Adapter	2680	Ethernet
6611 4-Port SDLC Adapter	2720	SDLC
6611 X.25 Adapter	2730	X.25

Figure 1-2. Sample Planning Chart

The following *IBM 6611 Network Processor Configuration Worksheets* show the parameters needed to configure the IBM 6611 number 1002 in Figure 1-1 on page 1-3

IBM 6611 Network Processor Configuration Worksheet

Completed by: J. Doe Date 6/26/92 Page 1 of 8

Complete one worksheet for each IBM 6611 — Name 1002 Slot 3

Note: Defaults are noted using a (†) and required information is noted using an (R).

EIA 422/449 Serial Adapter or V.35/V.36 Serial Adapter

Point-to-Point Protocol

Physical Interface Port _____
Enable interface: ☐ Enable† ☐ Disable
Cylink serial number (0-99999999): _____
Serial line speed (19200-204800 bps): _____
Data encoding: ☐ NRZI† ☐ NRZ
Local administered MAC address (R): _____

PPP

Enable PPP on this port:
☐ Enable† ☐ Disable
Maximum receive unit (octets): _____
Enable link quality monitoring:
☐ Enable ☐ Disable†
Link quality monitoring interval (usec): _____

LAN Bridging Protocol

Physical Interface Port _____
Enable Interface: ☐ Enable† ☐ Disable
Cylink serial number (0-99999999): _____
Serial line speed (1920-204800 bps): _____
Locally administered MAC address (R): _____

LAN Bridge Port Defaults

Enable LAN bridge PPP:
☐ Enable† ☐ Disable
Auto reboot on error:
☐ Enable† ☐ Disable
Performance counter threshold (0-9999): _____
Telecommunications link error threshold (0-9999): _____
Memory dump on error:
☐ Default drive† ☐ A drive ☐ B drive
☐ C drive ☐ D drive
Event log drive:
☐ Default drive† ☐ A drive ☐ B drive
☐ C drive ☐ D drive
Largest frame size:
☐ 516 ☐ 1500 ☐ 2052†

Network Management Parameters

Enable ring parameter server:
☐ Enable† ☐ Disable
Enable ring error monitor:
☐ Enable† ☐ Disable
Enable configuration report server:
☐ Enable† ☐ Disable
Passwords to link to network managers (up to 4 links):
PW 0: _____ PW 2: _____
PW 1: _____ PW 3: _____

Go to "Port-Level Protocol Parameters" to complete the adapter configuration.

Frame Relay

Physical Interface Port 1
Enable interface: ☒ Enable† ☐ Disable
Cylink serial number (0-99999999): _____
Serial line speed (19200-204800 bps): 1536000
Data encoding: ☒ NRZI† ☐ NRZ
Local administered MAC address (R): Router 3

Frame Relay

Enable frame relay on this port:
☒ Enable† ☐ Disable
Polling interval (seconds): _____
Fully enquiry interval (1-255): _____
LMI option:
☐ ANSI T1.617 Annex D
☐ LMIRev1
☐ None
Use Inverse ARP to resolve remote protocol addresses:
☒ Enable† ☐ Disable

List of DLCI Numbers for This Port

DLCIs assigned to this port (R):
15

Figure 1-3. Sample Configuration Worksheet

IBM 6611 Network Processor Configuration Worksheet	
Completed by: <u>J. Doe</u>	Date <u>6/26/92</u> Page <u>2</u> of <u>8</u>
Complete one worksheet for each IBM 6611 — Name <u>1002</u>	
Note: Defaults are noted using a (†) and required information is noted using an (R).	
System Configuration	
Routing—IPX Enable IPX router: ☒ Enable ☐ Disable† Split horizon for RIP filters: ☐ On† ☐ Poison reverse ☐ Off SAP Filters Status of all defined SAP filters: ☐ Enable† ☐ Disable Filtering mode: ☐ Deny† ☐ Permit	List of RIP Router Filters (continued) Network number (hex): _____ Host address to filter on: ☐ All Hosts† ☐ Enter Host Address Host address (hex): _____ Inbound RIP Filters Status of all defined inbound RIP filters: ☐ Enable† ☐ Disable Filtering mode: ☐ Deny† ☐ Permit

Figure 1-4. Sample Configuration Worksheet

IBM 6611 Network Processor Configuration Worksheet	
Completed by: <u>J. Doe</u>	Date <u>6/26/92</u> Page <u>3</u> of <u>8</u>
Complete one worksheet for each IBM 6611 — Name <u>1002</u>	Slot <u>3</u> Port <u>1</u>
Note: Defaults are noted using a (†) and required information is noted using an (R).	
Port-Level Protocol Parameters	
IPX Enable IPX routing on this port: ☒ Enable ☐ Disable† IPX network number (R): <u>0000 00E7</u> Destination host address (for PPP on a serial adapter) (R): _____ Encapsulation Method: (For Token-Ring Network 16/4 Adapter) ☐ Token-Ring 802.5† ☐ Token-Ring SNAP	List of Port Filters Filter ID (1-10) (R): _____ _____ _____ _____ Filter on packet type: ☐ Enable ☐ Disable† Pack type value (hex) (R): _____

Figure 1-5. Sample Configuration Worksheet

IBM 6611 Network Processor Configuration Worksheet

Completed by: J. Doe Date 6/26/92 Page 4 of 8

Complete one worksheet for each IBM 6611 — Name 1002

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Configuration

Bridging

Source Route Bridge

Enable source route bridging: ☒ Enable ☐ Disable †

Bridge number (0-15): 7

Designated ring number (hex) (R): 001

Spanning Tree Parameters

Bridge priority (hex): _____

Hello time (seconds): _____

Forward delay time (seconds): _____

Maximum age (seconds): _____

Data Link Switching

Data Link Switching

Enable forwarding of SNA traffic: ☐ Enable ☐ Disable †

☐ Enable ☐ Disable †

DLS

Protocols forwarded via DLS:

SNA ☐

Figure 1-6. Sample Configuration Worksheet

IBM 6611 Network Processor Configuration Worksheet

Completed by: J. Doe Date 6/26/92 Page 5 of 8

Complete one worksheet for each IBM 6611 — Name 1002

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Configuration

SNA

List of SNA Default Destinations

IP address of destination router (R): 9.0.0.1

Destination MAC address (hex) (R): 1000 5A10 0002

SNA Source Frame Filters

Status of all defined SNA source frame filters:

☐ Enable † ☐ Disable

Source frame filter type: ☐ Deny ☐ Permit †

List of SNA Source Frame Filters

Filter ID (1-100) (R): _____

Figure 1-7. Sample Configuration Worksheet

IBM 6611 Network Processor Configuration Worksheet	
Completed by: <u>J. Doe</u>	Date <u>6/26/92</u> Page <u>6</u> of <u>8</u>
Complete one worksheet for each IBM 6611 — Name <u>1002</u>	
Note: Defaults are noted using a (†) and required information is noted using an (R).	
System Configuration	
NetBIOS	
List of NetBIOS Default Destinations Destination name (R): <u>Router 4</u> _____ _____ _____ _____ IP address of destination router (R): <u>9.0.0.1</u> _____ _____ _____ _____	Source Name Filters Status of all defined source name filters: ☐ Enable† ☐ Disable Source name filter type: ☐ Deny ☐ Permit† List of NetBIOS Name Filters Source name (R): _____ _____ _____ _____

Figure 1-8. Sample Configuration Worksheet

IBM 6611 Network Processor Configuration Worksheet	
Completed by: <u>J. Doe</u>	Date <u>6/26/92</u> Page <u>7</u> of <u>8</u>
Complete one worksheet for each IBM 6611 — Name <u>1002</u> Slot <u>3</u> Port <u>1</u>	
Note: Defaults are noted using a (†) and required information is noted using an (R).	
Port-Level Protocol Parameters	
SNA Enable SNA frame forwarding on this port: ☒ Enable ☐ Disable† List of SAP Values for Frame Forwarding SAP Value (hex) (R): _____ _____ _____ _____	NetBIOS Forward NetBIOS frames on this port: ☒ Enable ☐ Disable† Forward NetBIOS datagram and datagram broadcast message on this port: ☐ Enable† ☐ Disable

Figure 1-9. Sample Configuration Worksheet

IBM 6611 Network Processor Configuration Worksheet

Completed by: J. Doe Date 6/26/92 Page 8 of 8

Complete one worksheet for each IBM 6611 — Name 1002 Slot 3 Port 1

Note: Defaults are noted using a (†) and required information is noted using an (R).

Port-Level Protocol Parameters

Source Route Bridge

Enable Source Route Bridging on this port:

☒ Enable ☐ Disable†

Ring number (hex)

(Not available for frame relay): _____

Maximum transmission unit (bytes):

- ☐ 516
☐ 1500
☐ 2052†
☐ 4472 (4 Mbps and 16 Mbps token-ring adapter only)
☐ 8144 (16 Mbps token-ring adapter only)
☐ 11407 (16 Mbps token-ring adapter only)
☐ 17800 (16 Mbps token-ring adapter only)

List of Ring Numbers to Frame Relay DLCI Numbers (frame relay only)

Ring Number (hex) (R):

004

DLCI number (R):

15

Spanning Tree Parameters

Spanning tree mode: ☐ Automatic† ☐ Manual

Path cost (0-65535) (for automatic only): _____

Enable forwarding of spanning tree packets (for manual only):

☐ Enable† ☐ Disable

Source Route Bridge Filters

Inbound Filters

MAC Address

Status of all defined inbound MAC address filters on this port:

☐ Enable† ☐ Disable

Filter Type: ☐ Deny† ☐ Permit

Frame Type: ☐ Single route broadcast (SRB)
☐ All routes broadcast (ARB)
☐ Both SRB and ARB†

List of Inbound MAC Address Filters (Source - Destination)

Frame Addresses

Source (R): _____

Destination (R): _____

Frame Address Masks

Source Mask: _____

Destination Mask: _____

Source SAP

Status of all defined inbound source SAP filters on this port:

☐ Enable† ☐ Disable

Filter Type: ☐ Deny† ☐ Permit

Frame type: ☐ Single route broadcast (SRB)
☐ All routes broadcast (ARB)
☐ Both SRB and ARB†

List of Inbound Source SAP Filters

Source SAP value (hex) (R): _____

SNAP Value

Status of all defined inbound SNAP filters on this port:

☐ Enable† ☐ Disable

Filter Type: ☐ Deny† ☐ Permit

Figure 1-10. Sample Configuration Worksheet

Configuration Considerations

General Recommendations for Configuration

You want to configure your network devices to form a unified network that functions correctly. Each device in your network must be configured so it is compatible with all other devices. To ensure compatibility throughout the network, it is recommended that a single individual or team define or approve the configuration for each network device, including each IBM 6611.

Use the Configuration Program to create a unique configuration for each IBM 6611 in your network. The configuration parameters for several IBM 6611s may be similar, and you may be tempted to modify one configuration to fit the other IBM 6611s. This is risky, and it is *not* advised. It is generally difficult to change a copy of one configuration into a configuration for another IBM 6611 without making errors. Remember, the IBM 6611s have different addresses, and often you must specify different parameters for each so that they are compatible.

It is recommended that all configurations and updates of your IBM 6611s be debugged and sent from a central control point. (Exceptions are the initial configurations, which must be loaded by diskette on your IBM 6611s.) This permits a single individual or team to monitor and test the network and coordinate network changes. See Chapter 14 on page 14-1 for information about sending configurations remotely to an IBM 6611.

Planning for Network Implementation

It is recommended that you implement your network in three phases: first, in a simulation network; second, in a limited segment of your real production network; and third, in your full production network.

Setting Up a Network for Simulation: Connect network devices, including your IBM 6611s, to form a network that closely resembles your real production network. Set up an IBM 6611 configuration workstation, and use it to configure each IBM 6611 for Internet Protocol (IP) only. Test the network to make sure IP connectivity has been established.

When you have established IP connectivity, configure each IBM 6611 for one additional protocol. Test the network to make sure this protocol is functioning correctly. Continue adding and testing one protocol at a time until you have successfully tested each of the protocols you plan to transport on your production network.

Finally, configure each IBM 6611 for all the protocols you plan to transport on your production network. Test the network to make sure all the protocols function correctly simultaneously.

Implementing a Limited Production Network: Once you have verified connectivity with a simulation network, you are ready for a limited production network implementation. Attach your IBM 6611s to an isolated segment of your production network, so that any adverse impact to your network will be limited to this segment. Try to perform this implementation at a time when it is not critical that this segment be functioning correctly.

As in the simulation network, first configure each IBM 6611 for IP only, and test the limited network to make sure IP connectivity has been established. Then configure

each IBM 6611 for one additional protocol and test the limited network to make sure this protocol functions correctly. Continue to add and test one protocol at a time until you have successfully tested all protocols you want to transport on your full production network.

Finally, configure each IBM 6611 for all the protocols you plan to transport on the full production network. Test the limited network to make sure all the protocols function correctly simultaneously.

Implementing Your Full Production Network: Once you have verified connectivity in a limited production network, you are ready for full production network implementation. Try to perform this implementation at a time when it is not critical that your production network be functioning correctly.

Repeat the procedures outlined in "Implementing a Limited Production Network" on page 1-10, adding and testing on your full network first IP, then each of the other protocols, and finally all the protocols together.

Configuration Trouble Shooting

Errors in the Configuration Program may cause different types of problems. A problem with configuration may appear initially to be a hardware problem because the IBM 6611 will not boot or data will not flow through an adapter port. In addition, problems with configuration may not result in an error initially; an error may occur only when specific conditions are encountered or when heavy network traffic occurs.

If you cannot resolve a problem after making a few changes to your configuration, generate a new configuration. Endless changes to a configuration often will compound the problem, whereas a new configuration can usually be generated and tested within a few hours.

Changing Configuration Parameters

Many of the IBM 6611 configuration parameters can be changed dynamically and do not require a machine restart. The configuration parameters are characterized according to the following categories:

- These parameters are fully dynamic.
- A restart of a particular function is required.
- A restart of the IBM 6611 is required.

Fully Dynamic Configuration Changes

The configuration parameters in this category are dynamic. Configuration changes do not require a restart at all. The changes are applied without disruption of current IBM 6611 operation within the network.

The following statements characterize the functions that can be changed dynamically:

- Adding any protocol except DECnet to any peer-capable adapter interface except for the EIA 422/449 Serial Adapter or the V.35/V.36 Serial Adapter
- Any parameter for LAN Bridging Protocol
- Protocol filters except DECnet, AppleTalk, and IP filters (including SNA, NetBIOS, transparent bridging, and source route bridging)
- IP functions except maximum transmission unit, Ethernet framing type, and IP filters (including addresses and netmasks)
- Any parameter associated with SNMP

- The IBM 6611 system management parameters (including EIA 232 serial ports, software lock, SNMP, userids and passwords, hosts, remote host names, and others)
- Parameters that are not listed in the tables starting in Table 1-22 on page 1-19 through Table 1-25 on page 1-21.

Configuration Changes Requiring the Function to Restart

The configuration parameters in this category are dynamic in the following way: the configuration changes do not require the IBM 6611 to be restarted, but the configuration changes do require that related functions be restarted. Several of these changes may be disruptive to the IBM 6611 operation within the network. However, dynamic recovery in the network can occur. When these parameters are changed after the initial configuration, the function in the IBM 6611 is restarted automatically when the configuration changes are applied.

The following statements characterize the functions that require the function to restart. A detailed list of parameters is in Table 1-1 through Table 1-22 on page 1-19.

- Any parameter associated with IP routing protocols (RIP, Hello, OSPF, BGP, EGP, import, export, static routes)
- Any parameter associated with data link switching except filters and list of data link switching participating routers
- Any parameter associated with an IBM Token-Ring Network Remote Bridge Point-to-Point Protocol
- Any parameter associated with bridge spanning tree function
- Any parameter associated with the SDLC Adapter
- Any parameter associated with X.25
- Any parameter associated with APPN nodes except port parameters.

Table 1-1. Configuration Parameters That Restart a Function — SRB

System-Level Source Router Bridging	
Enable source route bridging	page 3-4
Bridge number	page 3-4
Designated ring number	page 3-4
Bridge priority	page 3-5
Hello time	page 3-5
Forward delay time	page 3-5
Maximum age	page 3-5

Table 1-2. Configuration Parameters That Restart a Function — DLS

Data Link Switching Parameters	Page Reference
Enable forwarding of SNA traffic	page 3-25
Enable NetBIOS frame forwarding	page 3-25
Virtual ring segment number	page 3-25
Destination cache timeout	page 3-25
Default DLS IP Address for this IBM 6611	page 3-26
Accept connections only from specific 6611 routers	page 3-26
IP address of remote IBM 6611	page 3-26

Table 1-3. Configuration Parameters That Restart a Function — SNA

SNA Parameters	Page Reference
Status of all defined SNA source frame filters	page 3-27
Source frame filter type	page 3-28
Filter ID	page 3-28
Source address	page 3-28
Destination address	page 3-29
Destination address mask	page 3-29
Status of all defined SNA destination frame filters	page 3-29
Destination frame filter type	page 3-30
Source address mask	page 3-30

Table 1-4. Configuration Parameters That Restart a Function — SNA

SNA Port Parameters	Page Reference
Enable SNA frame forwarding on this port	page 6-49
SAP value	page 6-49

Table 1-5. Configuration Parameters That Restart a Function — NetBIOS

NetBIOS Port Parameters	Page Reference
Forward NetBIOS frames on this port	page 6-50
Forward NetBIOS datagram and datagram broadcast message on this port	page 6-50

Table 1-6 (Page 1 of 2). Configuration Parameters That Restart a Function — BGP

Border Gateway Protocol Parameters	Page Reference
Enable Border Gateway Protocol - BGP	page 3-67
Generate default route	page 3-68
Local autonomous system number	page 3-68
Default preference	page 3-68
Default metric	page 3-69
Autonomous system number (BGP group)	page 3-69
BGP group type	page 3-69
BGP group name	page 3-70
Metric out (BGP group)	page 3-70
Next hop destination (BGP group)	page 3-70
Interface IP address (BGP group)	page 3-71
Generate default route (BGP group)	page 3-71
Passive (BGP group)	page 3-71
Default network in (BGP group)	page 3-71
Default network out (BGP group)	page 3-72
Preference (BGP group)	page 3-72
Hold time (BGP group)	page 3-72
BGP neighbor IP address	page 3-73
BGP neighbor name (BGP configured neighbor)	page 3-73
Metric out (BGP configured neighbor)	page 3-73
Next hop destination (BGP configured neighbor)	page 3-73
Interface IP address (BGP configured neighbor)	page 3-74
Generate default route (BGP configured neighbor)	page 3-74
Passive (BGP configured neighbor)	page 3-75
Default network in (BGP configured neighbor)	page 3-75
Default network out (BGP configured neighbor)	page 3-75
Preference (BGP configured neighbor)	page 3-75
Hold time (BGP configured neighbor)	page 3-76
Unconfigured neighbor	page 3-76
BGP neighbor name (BGP unconfigured neighbor)	page 3-77
IP address (BGP unconfigured neighbor)	page 3-76
Mask (BGP unconfigured neighbor)	page 3-77

Table 1-6 (Page 2 of 2). Configuration Parameters That Restart a Function — BGP

Border Gateway Protocol Parameters	Page Reference
Enable BGP import filters	page 3-77
Import route filters	page 3-78
BGP import name	page 3-78
Autonomous system number (BGP import)	page 3-78
Autonomous system path specification	page 3-78
AS path origin	page 3-80
Restrict imports	page 3-81
Preference (BGP import)	page 3-81
Destination	page 3-81
Destination mask	page 3-82
Restrict routes	page 3-82
Preference (BGP import destination)	page 3-82

Table 1-7 (Page 1 of 2). Configuration Parameters That Restart a Function — EGP

Exterior Gateway Protocol Parameters	Page Reference
Enable OSPF	page 3-51
Router ID	page 3-51
Area ID	page 3-51
IP address	page 3-52
Interface type	page 3-55
IP address of neighbor router	page 3-55
Eligible to become a designated router	page 3-55
Enable RIP	page 3-58
Enable Exterior Gateway Protocol (EGP)	page 3-83
Local autonomous system number	page 3-83
Maximum initial packet size	page 3-83
Generate default route	page 3-83
Neighbor ASN	page 3-84
Maximum active neighbors	page 3-84
EGP group name	page 3-84
Preference	page 3-86
Default metric	page 3-86
Generate default routes from this neighbor	page 3-85
Import default route	page 3-85
Export default route	page 3-85
Minimum hello interval	page 3-85
EGP neighbor IP address	page 3-84
Minimum polling interval	page 3-85
Preference	page 3-83
Default metric	page 3-84
Default metric	page 3-86
Import default route	page 3-87
Export default route	page 3-87
Minimum hello interval	page 3-87
Minimum polling interval	page 3-87
Enable EGP import filters	page 3-88
Next hop address or domain name	page 3-87
Autonomous system number	page 3-88
Restrict	page 3-88
Preference	page 3-88
Destination	page 3-88
Destination mask	page 3-89
Restrict routes	page 3-89
Preference	page 3-89
Export selection name	page 3-95
To protocol	page 3-99
From protocol	page 3-95
Destination	page 3-95

Table 1-7 (Page 2 of 2). Configuration Parameters That Restart a Function — EGP

Exterior Gateway Protocol Parameters	Page Reference
Destination mask	page 3-95
Metric	page 3-96
Restrict	page 3-96
Type	page 3-99
Tag	page 3-99
AS number	page 3-99

Table 1-8. Configuration Parameters That Restart a Function — Hello

Hello Protocol Parameters	Page Reference
Enable Hello protocol	page 3-63
Broadcast	page 3-63
Route preference	page 3-63
IP address of source router	page 3-64
IP address of local interface	page 3-64
Listen for Hello updates	page 3-64
Send Hello updates	page 3-64
IP address of trusted router	page 3-64
Name of import filter	page 3-65
Destination	page 3-65
Destination mask	page 3-65
Preference	page 3-65
Restrict routes	page 3-65
Filter routes from	page 3-66
IP address of remote router	page 3-66
IP address of local interface	page 3-66

Table 1-9. Configuration Parameters That Restart a Function — IP

System-Level IP Parameters	Page Reference
Destination address	page 3-90
Destination mask	page 3-90
Next hop router	page 3-90
Preference	page 3-91
Retain route in master table	page 3-91

Table 1-10. Configuration Parameters That Restart a Function — IPX

System-Level IPX Parameters	Page Reference
Enable IPX router	page 3-102
Split horizon for RIP filters	page 3-102

Table 1-11. Configuration Parameters That Restart a Function — NetBIOS

System-Level NetBIOS Parameters	Page Reference
Destination name	page 3-47
Destination name filter type	page 3-49
Source name filter type	page 3-48
IP address of destination router	page 3-47
Status of all defined destination name filters	page 3-49
Status of all defined source name filters	page 3-48
NetBIOS Destination Name	page 3-50

Table 1-12 (Page 1 of 2). Configuration Parameters That Restart a Function — OSPF

Open Shortest Path First (OSPF) Parameters	Page Reference
Enable OSPF	page 3-51
Area ID	page 3-51

Table 1-12 (Page 2 of 2). Configuration Parameters That Restart a Function — OSPF

Open Shortest Path First (OSPF) Parameters	Page Reference
Area type	page 3-52
Stub cost	page 3-52
Authentication type	page 3-52
Interface IP address	page 3-52
Router priority	page 3-53
Router dead interval	page 3-54
Network number	page 3-55
Network mask	page 3-55
IP address of neighbor router	page 3-55
Eligible to become a designated router	page 3-55
Virtual neighbor ID	page 3-56
Transit area ID	page 3-56
Retransmit interval	page 3-56
Authorization key	page 3-56
Virtual link ID	page 3-56
Interface transit delay	page 3-57
Hello interval	page 3-57
Retransmit interval	page 3-56
Interface transit delay	page 3-57
Hello interval	page 3-57
Router dead interval	page 3-57
Authorization key	page 3-56
Cost	page 3-53
Poll interval	page 3-53
Interface type	page 3-55

Table 1-13. Configuration Parameters That Restart a Function — RIP Import

RIP Import Parameters	Page Reference
Name of import filter	page 3-60
Destination	page 3-60
Destination mask	page 3-60
Restrict	page 3-61
Preference	page 3-61
Filter routes from	page 3-61
IP address of remote router	page 3-61
IP address of local interface	page 3-62

Table 1-14. Configuration Parameters That Restart a Function — RIP

Routing Information Protocol (RIP) Parameters	Page Reference
Enable Routing Information Protocol (RIP)	page 3-58
Broadcast	page 3-58
Zero reserved fields	page 3-58
Route preference	page 3-59
IP address of local interface	page 3-59
Listen for RIP updates	page 3-59
Send RIP updates	page 3-60
IP address of trusted router	page 3-60
IP address of source router	page 3-59

Table 1-15 (Page 1 of 2). Configuration Parameters That Restart a Function — LAN Bridge

LAN Bridging Protocol Parameters	Page Reference
Performance counter threshold	page 5-12
Telecommunications link error threshold	page 5-12
Auto reboot on error	page 5-12

Table 1-15 (Page 2 of 2). Configuration Parameters That Restart a Function — LAN Bridge

LAN Bridging Protocol Parameters	Page Reference
Memory dump on error	page 5-13
Event log drive	page 5-13
Largest frame size	page 5-13
Enable LAN bridge protocol on this port	page 5-12
Enable ring parameter server	page 5-14
Enable ring error monitor	page 5-14
Enable configuration report server	page 5-14
Link password 0	page 5-14
Link password 1	page 5-15
Link password 2	page 5-15
Link password 3	page 5-15

Table 1-16. Configuration Parameters That Restart a Function — SRB Ports

Port-Level Source Route Bridging Parameters	Page Reference
Enable source route bridging on this port	page 6-5
Ring number	page 6-5
Ring Number	page 6-5
DLCI number	page 6-5
Spanning tree mode	page 6-6
Enable forwarding of spanning tree packets	page 6-7
Path cost	page 6-6
Maximum transmission unit	page 6-5
Designated ring number	page 3-4
Filter type	page 6-9
Status of all defined outbound source SAP filters on this port	page 6-20
Filter type	page 6-20
Frame type	page 6-20
Status of all defined inbound source SAP filters on this port	page 6-10
Filter type	page 6-11
Frame type	page 6-11
Status of all defined inbound ring number filters on this port	page 6-12
Filter type	page 6-12
Frame type	page 6-13
Status of all defined inbound MAC address filters on this port	page 6-9
Frame type	page 6-9
Hop count	page 6-27
Filter type	page 6-9
Status of all defined inbound SNAP filters on this port	page 6-11
Filter Type	page 6-12
Frame Type	page 6-28
Status of all defined outbound ring number filters on this port	page 6-22
Filter type	page 6-11
Frame type	page 6-11
Status of all defined outbound MAC address filters on this port	page 6-18
Filter type	page 6-18
Status of all defined outbound SNAP filters on this port	page 6-21

Table 1-17 (Page 1 of 2). Configuration Parameters That Restart a Function — IP/X.25

Port-Level IP/X.25 Parameters	Page Reference
Destination IP address for X.25	page 5-47

Table 1-17 (Page 2 of 2). Configuration Parameters That Restart a Function — IP/X.25

Port-Level IP/X.25 Parameters	Page Reference
Virtual circuit type	page 5-47
Logical channel number	page 5-47
Remote DTE address	page 5-47
Receive packet window size	page 5-48
Transmit packet window size	page 5-48
Closed user group index	page 5-49
Closed user group with outgoing access index	page 5-49
RPOA indices	page 5-49
User-defined facilities	page 5-48

Table 1-18. Configuration Parameters That Restart a Function — SDLC

SDLC Adapter Parameters	Page Reference
Enable interface	page 5-22
Physical link type	page 5-22
Serial encoding	page 5-23
Request to send	page 5-23
Data terminal ready	page 5-24
Data rate select	page 5-23

Table 1-19. Configuration Parameters That Restart a Function — SNA Ports

Port-Level SNA Parameters	Page Reference
SAP value	page 6-49
Enable SNA frame forwarding on this port	page 6-49

Table 1-20 (Page 1 of 2). Configuration Parameters That Restart a Function — X.25 Ports

Port-Level X.25 Parameters	Page Reference
Local DTE address (NUA)	page 5-33
Network identifier	page 5-33
Lowest logical channel number (incoming SVC)	page 5-34
Number of logical channels (incoming SVC)	page 5-35
Lowest logical channels (2-way SVC)	page 5-34
Number of logical channels (2-way SVC)	page 5-34
Lowest logical channel number (outgoing SVC)	page 5-33
Number of logical channels (outgoing SVC)	page 5-33
Lowest logical channel number (PVC)	page 5-34
Number of PVCs	page 5-35
Enable X.25	page 5-32
Calling address in incoming call packets	page 5-41
Auto-call unit	page 5-36
Auto-call unit disconnection timeout	page 5-37
CCITT support	page 5-35
SVC default receive packet size	page 5-38
SVC default transmit packet size	page 5-38
SVC default receive packet window	page 5-38
SVC default receive transmit packet window	page 5-38
T24 timer	page 5-46
T25 timer	page 5-46
Packet size and packet window size negotiation	page 5-41
Allow incoming calls	page 5-41
Allow outgoing calls	page 5-41
Allow fast select	page 5-43
Maximum number of reset packets	page 5-45
Maximum number of clear packets	page 5-45
Closed user group	page 5-45
Allow reverse charging	page 5-42

Table 1-20 (Page 2 of 2). Configuration Parameters That Restart a Function — X.25 Ports

Port-Level X.25 Parameters	Page Reference
Include calling address in call request packets	page 5-40
Packet size negotiation facility	page 5-41
Packet window size negotiation facility	page 5-42
CUG Basic format	page 5-43
CUG Extended format	page 5-43
CUG with OA selection facility — basic format	page 5-43
CUG with OA selection facility — extended format	page 5-44
CUG selection facility — basic format	page 5-43
CUG selection facility — extended format	page 5-43
Reverse charging/fast select facility	page 5-42
Frame window size	page 5-36
T1 timer	page 5-45
T4 timer	page 5-45
N2 counter	page 5-45
Connection mode	page 5-36
Poll timer	page 5-36
Frame modulo	page 5-36
Receive packet size	page 5-48
Transmit packet size	page 5-48
Receive packet window size	page 5-48
Transmit packet window size	page 5-48
PVC logical channel number	page 5-37
PVC receive packet size	page 5-37
PVC transmit packet size	page 5-38
PVC Receive packet window	page 5-38
PVC Transmit packet window	page 5-38
Autoreset value	page 5-39

Table 1-21. Configuration Parameters That Restart a Function — SNA Stations

SNA Station Parameters	Page Reference
Station address	page 5-25
Station token-ring source address	page 5-25
Station token-ring destination address	page 5-26
Transmit window count	page 5-28
Retransmit count	page 5-27
Retransmit threshold (frames)	page 5-27
Force disconnect timeout	page 5-29
Maximum I-field size	page 5-28
Primary repoll timeout	page 5-29
Primary repoll count	page 5-28
Primary repoll threshold	page 5-27
Primary slow list timeout	page 5-27
Station token-ring source SAP	page 5-25
Station token-ring destination SAP	page 5-26
Station XID Value	page 5-26

Table 1-22 (Page 1 of 2). Configuration Parameters That Restart a Function — APPN Parameters

APPN Parameters	Page Reference
Network ID	page 3-34
Control point name	page 3-34
Accept connection requests from any node	page 3-35
XID ID number (of node)	page 3-35
Maximum number of network nodes in your APPN network	page 3-44
Maximum number of end nodes and LEN nodes serviced by this node	page 3-44

Table 1-22 (Page 2 of 2). Configuration Parameters That Restart a Function — APPN Parameters

APPN Parameters	Page Reference
Average number of LUs associated with end nodes and LEN nodes serviced by this node	page 3-44
Maximum cached directory entries	page 3-46
Maximum shared memory	page 3-45

Table 1-23. Configuration Parameters That Restart AppleTalk on Affected Port-Only (Valid for Ethernet and Token-Ring Ports)

AppleTalk Parameters	Page Reference
Enable AppleTalk routing on this port	page 6-60
Network number range (of locally-attached network)	page 6-60
Default zone name	page 6-61
Starting value for node ID acquisition	page 6-61
Enable security filters	page 6-62
Enable network number range filter	page 6-62
Network number range (for network number range filter)	page 6-63
Additional zone name (add name)	page 6-62
Accept routing information	page 6-64
Network number range (add selected network)	page 6-65
Enable network number range filter (for selected networks)	page 6-65
Network number range (for selected networks filter)	page 6-66
Allowable zone name (add name for selected network)	page 6-66

Configuration Changes Requiring the IBM 6611 to Restart

The configuration parameters in this category are not dynamic. The configuration changes require the IBM 6611 to be restarted. If any of these configuration parameters are changed after the initial configuration, the IBM 6611 is restarted automatically (equivalent to the function of the Reset key) when the configuration changes are applied.

The following statements explain the functions that require a machine restart. A detailed list of parameters is in Table 1-24 on page 1-21 through Table 1-30 on page 1-22.

- Any parameter associated with a DECnet** protocol
- Any IPX parameter related to Point-to-Point Protocol (PPP)
- Any XNS** parameter related to PPP
- Any parameter associated with PPP
- Any parameter associated with frame relay
- Any parameter associated with physical interfaces or ports on peer-capable adapters (EIA 422/449 Serial Adapter, V.35/V.36 Serial Adapter, Token-Ring Network 16/4 Adapter, or Ethernet Adapter)
- Removing any protocol from a peer-capable adapter interface except source route bridging and IBM Token-Ring Network Bridge Program Point-to-Point Protocol
- IP filters
- Maximum transmission unit
- Ethernet framing type (802.3 or Ethernet Version 2).

Table 1-24. Configuration Parameters That Restart the IBM 6611 — DECnet

System-Level DECnet Parameters	Page Reference
Enable DECnet router	page 3-116
Local DECnet address	page 3-116
Node type	page 3-116
Area maximum cost	page 3-117
Area maximum hops	page 3-117
Maximum address	page 3-118
Maximum area	page 3-118
Maximum cost	page 3-117
Maximum hops	page 3-117
Maximum visits	page 3-118
Maximum broadcast non-routers	page 3-119
Maximum broadcast routers	page 3-118
Buffer size	page 3-119
Filter ID	page 3-120
Filter type	page 3-120
Permit or deny traffic	page 3-120
Filter DECnet address 1	page 3-120
Filter mask 1	page 3-121
Filter DECnet address 2	page 3-121
Filter mask 2	page 3-121

Table 1-25. Configuration Parameters That Restart the IBM 6611 — DECnet Ports

Port-Level DECnet Parameters	Page Reference
Enable DECnet on this interface	page 6-82
Circuit cost	page 6-82
Hello timer	page 6-82
Router priority	page 6-83
Routing timer	page 6-83
Maximum routers	page 6-83
Filter ID	page 6-84
Direction in which packet is moving	page 6-85
Status of all defined DECnet filters on this port	page 6-84
DLCI number	page 6-83

Table 1-26. Configuration Parameters That Restart the IBM 6611 — Ethernet Adapter

Ethernet Adapter Parameters	Page Reference
Enable interface	page 5-6
MAC address	page 5-6
Alternate Ethernet MAC address	page 5-7
Allow multicasting	page 5-7

Table 1-27. Configuration Parameters That Restart the IBM 6611 — Frame Relay

Frame Relay Parameters	Page Reference
Enable frame relay on this port	page 5-19
DLCIs assigned to this port	page 5-20
Polling interval	page 5-19
Full inquiry interval	page 5-19
LMI option	page 5-19
Use InARP to resolve remote protocol addresses	page 5-20

Table 1-28 (Page 1 of 2). Configuration Parameters That Restart the IBM 6611 — PPP

Point-to-Point Protocol Parameters	Page Reference
Enable point-to-point protocol (PPP) on this port	page 5-16
Maximum receive unit	page 5-16

Table 1-28 (Page 2 of 2). Configuration Parameters That Restart the IBM 6611 — PPP

Point-to-Point Protocol Parameters	Page Reference
Enable link quality monitoring	page 5-16
Link quality monitoring interval	page 5-17

Table 1-29. Configuration Parameters That Restart the IBM 6611 — serial adapter

**Serial Adapter Parameters (EIA 422/449 Serial Adapter,
V.35/V.36 Serial Adapter)**

Enable interface	page 5-10
Data link protocol	page 5-9
Cylink serial number	page 5-10
Data encoding	page 5-11
Locally administered MAC address	page 5-11
Serial line speed	page 5-10

Table 1-30. Configuration Parameters That Restart the IBM 6611 — Token-Ring Network 16/4 Adapter

Token-Ring Adapter Parameters	Page Reference
Enable interface	page 5-3
MAC address	page 5-3
Locally administered address	page 5-4
Token-ring data rate	page 5-5
MAC address format	page 5-4
Broadcast type	page 5-5

Table 1-31. Configuration Parameters That Restart the IBM 6611 — Transparent Bridging

Transparent Bridging Parameters	Page Reference
Enable transparent bridging (system-level parameter)	page 3-11
Enable transparent bridging on this port (port-level parameter)	page 6-29

Table 1-32. Configuration Changes That Restart the IBM 6611 — AppleTalk

AppleTalk Parameters	Page Reference
Additional zone name (change or remove name)	page 6-62
Network number range for selected networks (change or remove)	page 6-65
Allowable zone name for selected networks (change or remove)	page 6-66
Port type	page 6-60

Chapter 2. Using the Configuration Program

Introduction to the Configuration Program	2-2
Using the Configuration Program on a RISC System/6000 Workstation	2-3
Hardware and Software Requirements	2-3
Installing the Configuration Program	2-3
Starting the Configuration Program	2-4
Using the Configuration Program on a PS/2 Workstation	2-5
Hardware and Software Requirements	2-5
Installing the Configuration Program	2-5
Starting the Configuration Program	2-6
Operating the Configuration Program	2-6
The Main Window	2-7
The Menu Bar	2-9
Creating an IBM 6611 Configuration File	2-9
Transporting the Configuration File to the IBM 6611	2-13
Transporting the File Using a Diskette	2-13
Transporting the File without Using a Diskette	2-13
Direct IP Connection	2-14
The Modem Transfer Method	2-14
The FTP Transfer Method	2-14

Introduction to the Configuration Program

The Configuration Program provides a graphical user interface that allows you to configure the IBM 6611. The interface is based on OSF/Motif. The Configuration Program can be run on either of the following workstations:

- RISC System/6000 workstation
- Personal System/2 (PS/2) workstation.

On the RISC System/6000 workstation, the Configuration Program uses AIXwindows*. On the PS/2 workstation, the Configuration Program uses Microsoft Windows**. Before using the Configuration Program, you should fill out the IBM 6611 Network Processor Configuration Worksheets (*Configuration Worksheets*) in Appendix A. See Chapter 3 through Chapter 6 for information about the configuration parameters.

Store the Configuration Program diskettes in the binder for this book. The Configuration Program diskettes contain a README file for quick reference. The README file contains information that is also contained in this book.

When you install the Configuration Program, several files are copied to the installation directory, *cfg*. The files that are copied vary according to the type of workstation you are using. If you want to change the name of the installation directory, enter the name you prefer before installing the Configuration Program files. The following lists provide the file names for each type of workstation:

- AIXwindows workstations
 - README
 - cfg.aix
 - cfg.app
 - cfg.hlp
 - cfg.msg
 - cfg
 - cfg.ini (aix.ini is located on Configuration Program Diskette 1)
 - cfg.lgo
- Microsoft Windows 3.0 workstations
 - README
 - cfg.exe
 - cfg.app
 - cfg.hlp
 - cfg.msg
 - cfg.ini (win30.ini is located on Configuration Program Diskette 2)
 - cfg.lgo
 - winmem32.dll
- Microsoft Windows 3.1 workstations
 - README
 - cfg.exe
 - cfg.app
 - cfg.hlp
 - cfg.msg
 - cfg.ini (win31.ini is located on Configuration Program Diskette 3)
 - cfg.lgo
 - winmem32.dll

Note: The Configuration Program uses the user defaults file, *cfg.ini*, to perform startup actions while loading the runtime image. Although this file can be edited manually using a text editor, such as *vi*, IBM recommends that you make changes to the user defaults file by using the User Preference window. The *ini* file will be written when you select the OK push button. If *cfg.ini* is not in the installation directory, the default attributes are used.

You need special fonts to run the IBM Multiprotocol Network Program Configuration Program. From an AIX window, use the command **xset -q** to access the fonts.

This chapter explains the tasks you perform to configure the IBM 6611:

- Installing the Configuration Program
- Starting the Configuration Program
- Operating the Configuration Program
- Transporting the configuration file to the IBM 6611.

Using the Configuration Program on a RISC System/6000 Workstation

This section describes how to use the Configuration Program on a RISC System/6000 workstation.

Hardware and Software Requirements

The following hardware and software are required to operate the Configuration Program on the RISC System/6000 workstation:

- AIX* 3.1.5 or later with Transmission Control Protocol/Internet Protocol (TCP/IP) enabled
- AIXwindows
- 16 MB of memory
- 1.44-MB, 3.5-inch diskette drive
- 10 MB of available space on the fixed disk drive
- Graphics display
- Mouse.

Installing the Configuration Program

To install the Configuration Program on a RISC System/6000 workstation:

- Step 1** Log in to AIX as a non-root user.
- Step 2** Place Diskette 1 in the 3.5-inch diskette drive.
- Step 3** At the AIX prompt, type the following commands:

Note: AIX is case-sensitive.

dosread -a install.aix install.aix

Where:

<code>dosread</code>	Reads the file from a DOS diskette and places it in the current directory.
<code>-a</code>	Converts the DOS file to an AIX file.
<code>install.aix</code>	The file name on the diskette.
<code>install.aix</code>	The file name to be used in the AIX system.

Then type:

`chmod 550 install.aix`

<code>chmod</code>	Changes the file permissions given to the owner and group.
<code>550</code>	Defines the permission types for a user, group, and other users. In this case, the user and group are allowed read and execute permission, and others are allowed only read permission.
<code>install.aix</code>	The name of the file for which you are changing the permissions.

Step 4 Type **`install.aix`** at the AIX prompt and press Enter.

Step 5 Follow the prompts that appear on the screen to complete the installation.

Note: When you press the Num Lock key on AIX 3.2 workstations, the Configuration Program does not process input from the mouse or the keyboard. The Configuration Program will appear to be suspended. To stop the suspension, release the Num Lock key.

Starting the Configuration Program

The following are considerations that discuss starting the Configuration Program.

- X-Windows must be running on the RISC System/6000 workstation before starting the Configuration Program. (Type **`xinit`** to start X-Windows.)
- `X11fnt.coreX.fnt` must be installed to have access to the M.I.T X11.4 (75 DPI and 100 DPI) fonts.
- When using an xterm screen, change the current directory to the directory containing the Configuration Program files. For example, type **`cd cfg`**. Then, type **`cfg`**. The Configuration Program appears on the screen.
- Sometimes Configuration Program windows are positioned close to the upper left corner of the window instead of the upper left corner of the window border.

To correct this problem on RISC System/6000 workstations using Open Look windows, place the following information in the `$HOME/.Xdefaults` file:

```
Cfg6611.normal.mappingOffset: 5,26
Cfg6611.transient.mappingOffset: 5,5
Cfg6611.normal.configurationOffset: 0,0
Cfg6611.transient.configurationOffset: 0,0
```

To correct this problem on RISC System/6000 workstations using the OSF/Motif window manager, the following offsets are recommended:

```
Cfg6611.normal.mappingOffset: 11,27
Cfg6611.transient.mappingOffset: 11,27
Cfg6611.normal.configurationOffset: 0,0
Cfg6611.transient.configurationOffset: 0,0
```

- As part of the installation, the Configuration Program uses the **dosread**, **doswrite**, and **dosdir** commands. The Configuration Program also uses these commands to read and write configurations to the diskette drive. These commands must be installed on the RISC System/6000 workstation before you install and use the Configuration Program.

After you have started the Configuration Program, see “Operating the Configuration Program” on page 2-6 for instructions.

Using the Configuration Program on a PS/2 Workstation

This section describes how to use the Configuration Program on a PS/2 workstation.

Hardware and Software Requirements

The following hardware and software are required to use the Configuration Program on a PS/2 workstation using an Intel** 80386** or higher processor or a compatible system which has an Intel 80386 or higher processor and is equipped with:

- IBM DOS 3.2 or later, MS-DOS** 3.3 or later
- Microsoft Windows 3.0 or later
- 8 MB of memory
- 1.44-MB, 3.5-inch diskette drive
- 10 MB of available disk space on the disk drive
- 8514 Graphics Adapter (VGA) display, either monochrome or color
- Mouse.

Installing the Configuration Program

Figure 2-1 shows the Configuration Program Installation panel.

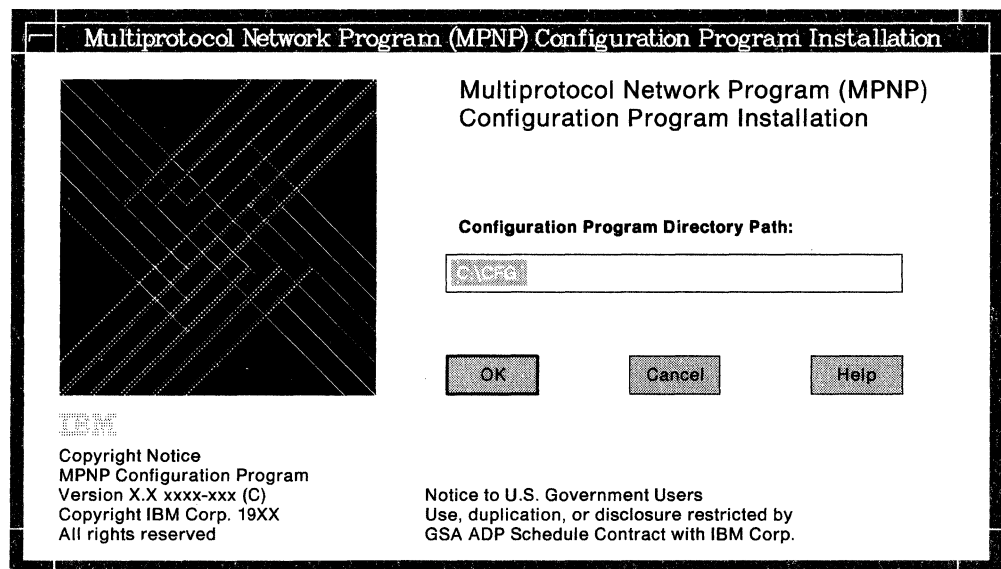


Figure 2-1. Configuration Program Installation Screen

To install the Configuration Program on a PS/2 workstation:

- Step 1** Type **win** beside the DOS prompt to start Windows.
- Step 2** Place Diskette 1 in the diskette drive.
- Step 3** Select **File** from the menu bar.
- Step 4** Select **Run** from the pull-down window.
- Step 5** Type **a:install** on the command line and select **OK** to start the installation.
- Step 6** Follow the prompts that appear on the screen.

After a successful installation, an icon labeled *6611 Configuration* will be added to the Main program group.

Note: In a subsequent installation, a second icon labeled *6611 Configuration* is added to the Main program group. To delete one of the icons, follow these steps:

- Step 1** Select the icon that you want to delete.
- Step 2** Select **File** from the menu bar.
- Step 3** Select **Delete** from the cascade menu.
- Step 4** An information message window is displayed. Select **Yes** to delete the icon.

Starting the Configuration Program

To start the Configuration Program on a PS/2 workstation, click on the icon representing the Configuration Program.

Operating the Configuration Program

Operating the Configuration Program is the same on a PS/2 workstation or RISC System/6000 workstation. When you run the Configuration Program, other files are created in the installation directory. File names with the extension *cdb* are created when you request the Configuration Program to create or save a configuration.

Note: These configuration files are in binary format and must not be changed using a text editor.

A file named *config* may also appear in the installation directory. The Configuration Program creates this file when you create an IML diskette. First, the Configuration Program creates the configuration file. Then, the Configuration Program copies the files to the diskette. If a file named *config* already exists, the Configuration Program replaces the existing file with the new one.

The following sections describe the Configuration Program main window and describe how to create a configuration file using the Configuration Program.

After selecting the 6611 Configuration Program icon, the panel shown in Figure 2-2 on page 2-7 is displayed.

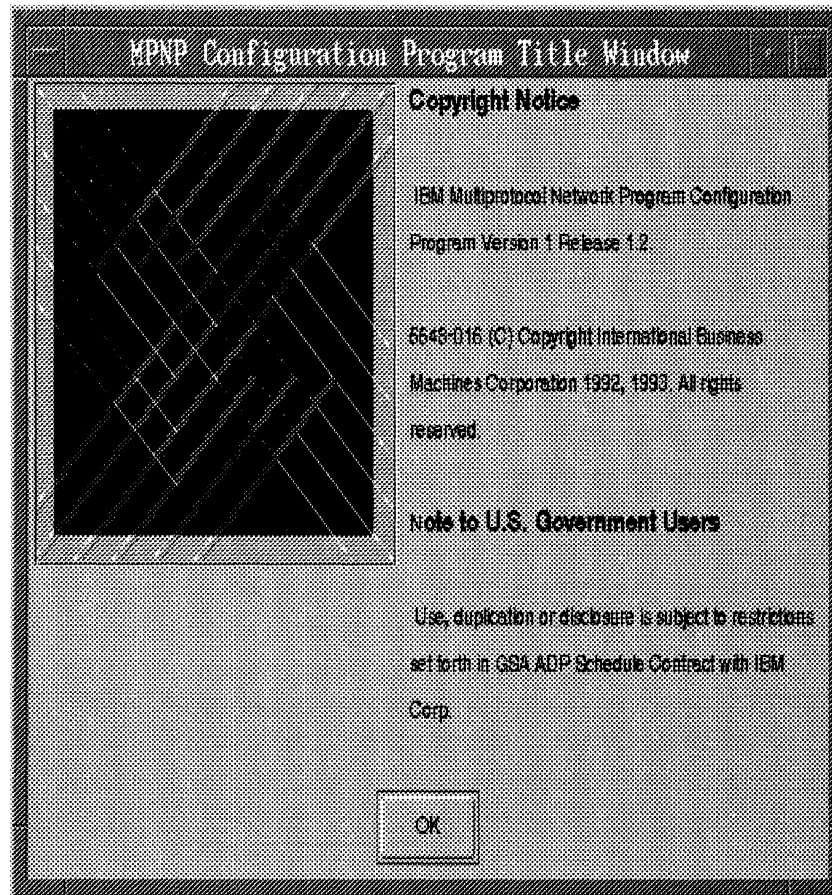


Figure 2-2. Configuration Program Logo Screen

The Main Window

The first window that you see after the copyright panel is the main window (**MPNP Configuration Program**). Figure 2-3 on page 2-8 illustrates the main window.

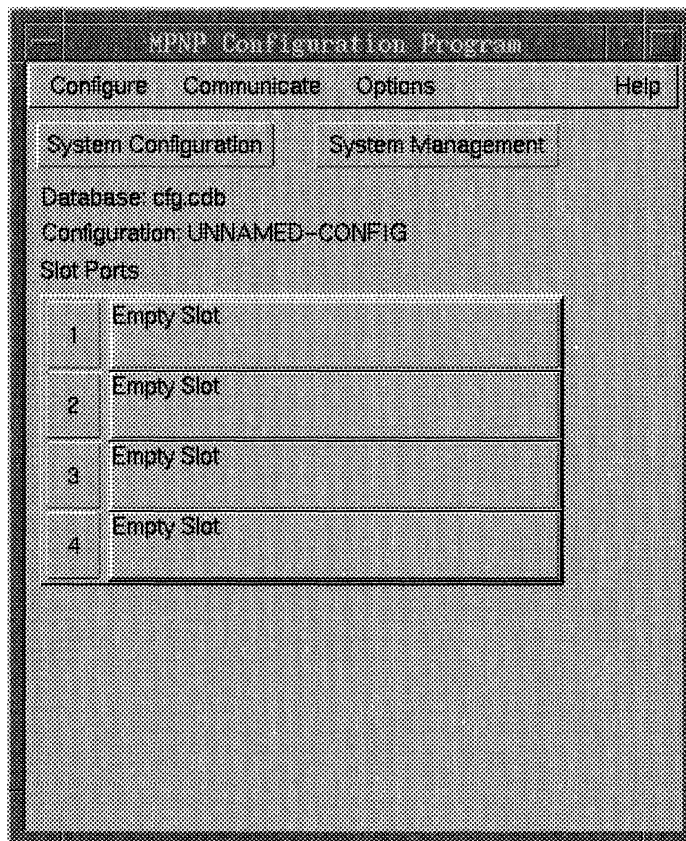


Figure 2-3. Main Window of the Configuration Program

On the main window, you see:

- The menu bar, which contains the following options:
 - Configure
 - Communicate
 - Options
 - Help
- Four adapter slots that represent the Model 140.

Four slots is the default. You can change the window to display 2 slots to represent the Model 120, or 7 slots to represent the Model 170. (Refer to “Creating an IBM 6611 Configuration File” on page 2-9 for configuration steps.)

The Menu Bar

Table 2-1 lists the choices available under each selection on the menu bar. The menu bar includes the following options:

Table 2-1. MPNP Configuration Program Menu Bar

Configure	Communicate	Options	Help
New configuration...	Send configuration...	Set font...	On Windows
Open configuration...	Retrieve...	Set colors...	On Keys
Save configuration...	Delete...	Set default model...	Index
Save configuration as...		Set validity checking...	On Help
Delete configuration...		Trace configuration R/W...	On Version
Write IML file to file...		Port Summary...	On Trademarks
Create configuration diskette			Tutorial
Read configuration diskette			
Copy from another configuration database			
Exit			

Creating an IBM 6611 Configuration File

Follow these steps to create a configuration file for an IBM 6611:

- Step 1** At the main window, verify that the correct model of the IBM 6611 is displayed. If you want to configure a Model 120 (2 slots) or Model 170 (7 slots), but a Model 140 (4 slots) is displayed, follow these steps:
1. Select **Configure** from the menu bar.
 2. Select **New configuration** from the cascade menu.
 3. Select **Model 120** or **Model 170** from the cascade menu.

Step 2 Use System Configuration to configure the routing, bridging, and data link switching functions that you want the IBM 6611 to perform.

Figure 2-4 illustrates the System Configuration window.

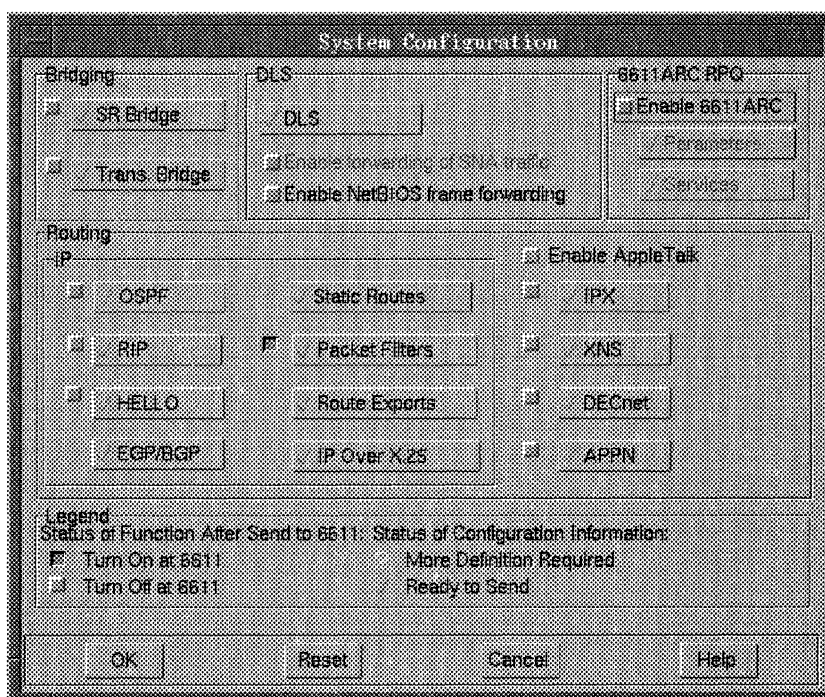


Figure 2-4. System Configuration Window

Step 3 Configure the **System Management** parameters. Use System Management to specify:

- The host name and domain name for the IBM 6611
- Baud rate for the S1 and S2 serial ports
- Lock value of the Multiprotocol Network Program
- SNMP network management information
- Controlling and viewing userids and passwords for the IBM 6611
- The time when a configuration file is to be applied to the system
- List of hosts that can configure the IBM 6611 from the Configuration Program
- Mapping of host names to IP addresses
- Name and time servers on the network that you want the IBM 6611 to use.

Figure 2-5 on page 2-11 illustrates the System Management window.

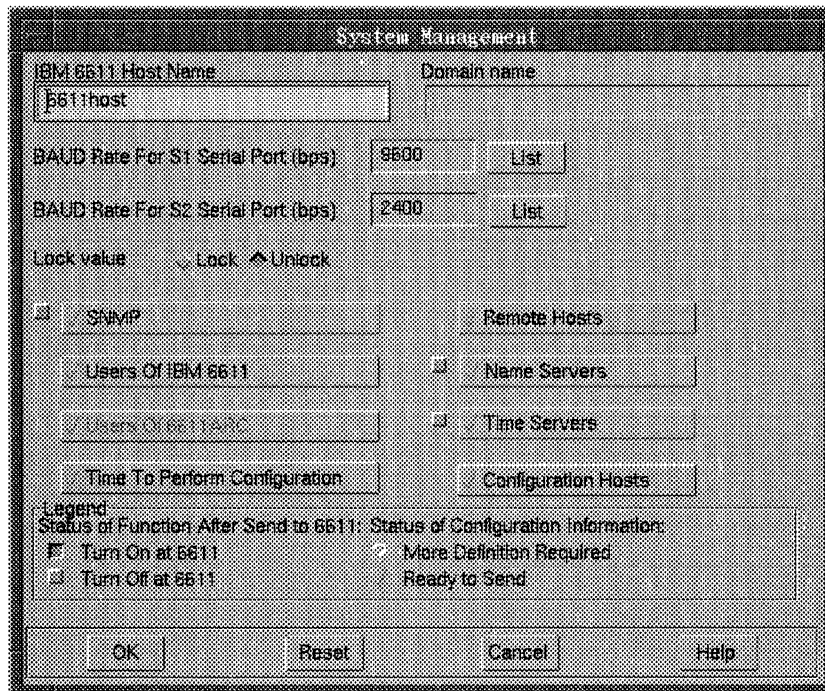


Figure 2-5. System Management Window

Step 4 To display the Port Summary window:

Step 1 Select **Options** from the menu bar.

Step 2 Select **Port Summary** from the cascade menu.

This window displays current configuration information about the adapters and protocols for each adapter slot. This window updates the configuration of the adapters and protocols as you continue the configuration process. Figure 2-6 illustrates the Port Summary window.

Port Summary						
Slot	Port	Bridge	SNA	Netbios	Protocols Routed	Protocols Discarded
1 EN 2 4 Port	1	No				IP,IPX,XNS
	2	No				
	3	No				
	4	No				
3 TR	1	No	No	No		IP,IPX,XNS
4 X.25	1	No	No	No	IP	IPX,XNS,D

Figure 2-6. Port Summary Window

Step 5 Configure the adapter slots. Select an adapter slot by clicking on the numbered push button that corresponds to the slot that you want to configure. (You cannot select the physical slot.) A pop-up menu appears that allows you to add an adapter. The other actions (delete, move, and swap) cannot be selected when the adapter slot is empty.

When you select **Add**, a cascade menu appears. Click on the name of the adapter you want to add from the cascade menu. Your choices are as follows:

- Token Ring
- Ethernet
- Serial (EIA 422/449 Serial Adapter and V.35/V.36 Serial Adapter)
- SDLC Adapter
- X.25.

Step 6 Configure the adapter ports. The serial adapters and the SDLC Adapter have more than one port. You must configure each port that will be used.

To configure a port, select the port by clicking on the port push button. A window appears with a number of selections. If the panel that appears has the **Physical interface** push button, select the **Physical interface** push button to configure the adapter parameters. Proceed to configure the port-level parameters for the adapter port. Repeat this step for each port that will be used.

Figure 2-7 illustrates the port-level parameters window.

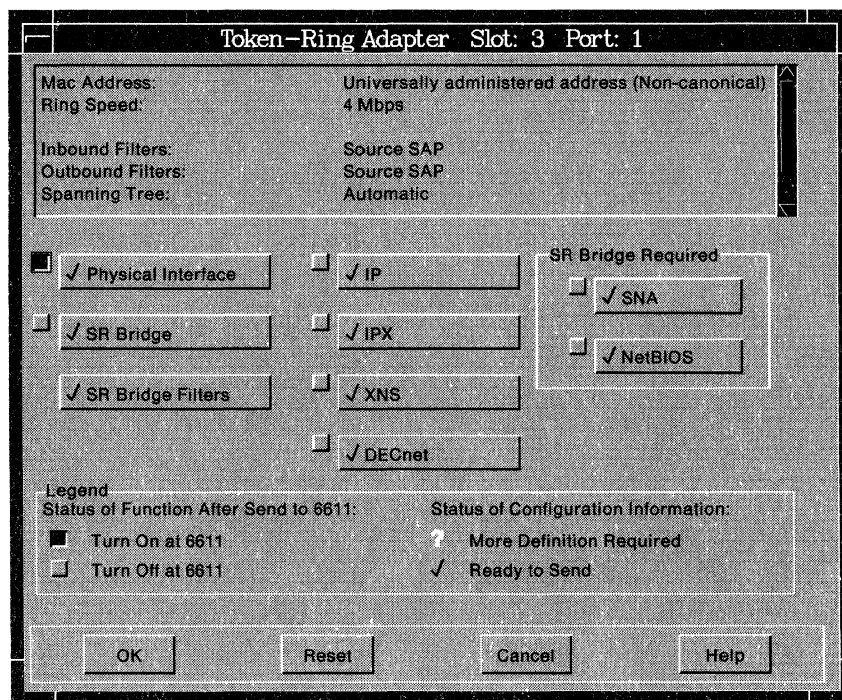


Figure 2-7. Port-Level Parameters Window

Step 7 After you have configured all of the functions and protocols that you want enabled for the IBM 6611, save the configuration file. At the main window, select **Configure** and then select the **Save** or **Save as ...** option to save the file.

Continue with “Transporting the Configuration File to the IBM 6611” for instructions on how to transport the file.

Transporting the Configuration File to the IBM 6611

After you have created a configuration file using the Configuration Program, you must transport the file to the IBM 6611. You may transport the file using a diskette or using a network connection to the IBM 6611.

Note: The preferred method to transport the initial configuration is to carry the diskette to the IBM 6611 and place it in the diskette drive. Then, turn the power switch to **On**. See “Transporting the File Using a Diskette” for more instructions.

Transporting the File Using a Diskette

After you have created a configuration file using the Configuration Program, you can transport the file to the IBM 6611 using a diskette. Follow these steps to create a configuration diskette and load the diskette on the IBM 6611:

1. Select **Configure** from the menu bar of the Configuration Program main window.
2. Select **Create configuration diskette** from the cascade menu. Enter the information that the program needs to copy the file to the desired drive.
3. Carry the configuration diskette to the IBM 6611 and place it in the diskette drive.
4. To read the configuration file, set the IBM 6611 keymode switch to **Normal** and then set the power switch to **On**.

The configuration process installs the configuration parameters and uses those parameters as the current configuration.

5. Observe the 3-digit display while the configuration process reads the file. See Appendix B for an explanation about the codes that are displayed. When the configuration process has read the file and initialized the IBM 6611, the code c89 is displayed on the 3-digit display.
6. After the configuration process has completed, remove the diskette from the drive.

Note: The diskette drive will be read when a power-on reset (POR) occurs.

Warning: You must remove the diskette to prevent the diskette from being read accidentally during a subsequent configuration of the IBM 6611. Removing the diskette also prevents accidentally overwriting the configuration file on the diskette.

Transporting the File without Using a Diskette

After you have created a configuration file using the Configuration Program, you may use one of three methods to transport the file over a network connection to the IBM 6611.

Direct IP Connection

You can send a file directly from the Configuration Program workstation to an IBM 6611 provided that:

- The workstation is a RISC System/6000 workstation which has a network connection to the IBM 6611 and the IBM 6611 is active on the network.
- For the initial configuration, a minimal configuration must be installed on the IBM 6611. See "Initial Configuration without Using a Diskette" on page 14-11 for instructions about how to perform a minimal configuration.

Note: All adapters that are in the IBM 6611 must be configured in order to use the **Send configuration** function. If there are adapters in your IBM 6611 that you do not want to use, you must still define them in the configuration. Then, go into the slot level configuration and disable everything that defaults to enable for the adapters that you do not want to use.

Use the following procedure to send the configuration file from the RISC System/6000 workstation to the IBM 6611:

1. Select **Communicate** from the menu bar of the Configuration Program main window.
2. Select **Send configuration** from the cascade menu. Enter the information that the program needs to send the file to the desired IBM 6611.

The IBM 6611 will automatically process the configuration file upon receipt.

The Modem Transfer Method

You can send a configuration file from a remote workstation to an IBM 6611 using a modem connection. The following conditions must be met:

- The workstation must be connected using a modem to the IBM 6611 through one of its EIA 232 serial ports.

The workstation can be connected using a modem to another node on the same network as the IBM 6611 provided that the other node supports RLOGIN and has a network connection to the IBM 6611. The IBM 6611 must be active on the network.

- The workstation supports outgoing calls and the Xmodem protocol.

See "Modem Transfer Method" on page 14-12 for instructions about how to send a configuration file using this method.

The FTP Transfer Method

You can send a configuration file from a remote workstation to an IBM 6611 using FTP over an IP network. The following conditions must be met:

- For initial configuration, a minimal configuration must be installed on the IBM 6611 and the IBM 6611 is active on the IP network. See "Initial Configuration without Using a Diskette" on page 14-11 for instructions about how to perform a minimal configuration.
- The workstation is active on the IP network and supports FTP.

See "FTP Transfer Method" on page 14-14 for instructions about how to send a configuration file using this method.

Chapter 3. System Configuration Parameters

About this Chapter	3-3
Source Route Bridging	3-4
Spanning Tree Parameters	3-5
Port Filter Order	3-6
Transparent Bridging	3-10
Filtering Database Parameters	3-12
Static Destination Address Filters	3-12
Port Filter Order	3-13
Spanning Tree Parameters	3-16
Data Link Switching	3-18
Configuring Data Link Switching	3-19
Enable Protocols Forwarded by Data Link Switching	3-25
Data Link Switching Specific Parameters	3-25
List of Data Link Switching Partners	3-26
Systems Network Architecture (SNA)	3-27
List of SNA Default Destinations	3-27
SNA Frame Filters	3-27
Source Frame Filters	3-27
List of SNA Source Frame Filters	3-28
Destination Frame Filters	3-29
List of Destination Frame Filters	3-30
Advanced Peer-to-Peer Networking	3-32
Configuring an IBM 6611 Network Node	3-32
Network Node Configuration	3-34
Data Link Switching Connection	3-36
Address of This Node for Data Link Switching	3-36
Adjacent Node Definitions (Data Link Switching)	3-37
IP Connection	3-41
Adjacent Node Definitions	3-41
Tuning an IBM 6611 Network Node	3-43
NetBIOS	3-47
List of NetBIOS Default Destinations	3-47
NetBIOS Name Filters	3-48
NetBIOS Source Name Filters	3-48
List of NetBIOS Source Name Filters	3-48
NetBIOS Destination Name Filters	3-49
List of NetBIOS Destination Name Filters	3-49
IP Routing Protocols	3-51
OSPF	3-51
List of OSPF Areas	3-51
List of OSPF Interfaces	3-52
List of OSPF Neighbors	3-55
OSPF List of Network Ranges	3-55
OSPF List of Virtual Links	3-56
Routing Information Protocol	3-58
List of RIP Source Routers	3-59
RIP Interface Settings	3-59
List of RIP Trusted Routers	3-60
List of RIP Imports	3-60
List of RIP Import Destinations	3-60
List of RIP Import Routers	3-61
List of RIP Import Interfaces	3-62

Hello Protocol	3-63
List of Hello Source Routers	3-64
Hello Interface Settings	3-64
List of Hello Trusted Routers	3-64
List of Hello Imports	3-65
List of Hello Import Destinations	3-65
Hello Import Routers	3-66
List of Hello Import Interfaces	3-66
Border Gateway Protocol (BGP)	3-67
BGP Global Default Parameters	3-67
BGP Group Parameters	3-69
BGP Neighbor Parameters	3-73
Configured Neighbor Parameters	3-73
Unconfigured Neighbor Parameters	3-76
BGP Import Filters	3-77
List of BGP Imports	3-78
Exterior Gateway Protocol (EGP)	3-83
List of EGP Groups	3-84
List of EGP Neighbors	3-84
EGP Group Options	3-86
EGP Imports	3-88
List of EGP Imports	3-88
List of EGP Import Destinations	3-88
Static Routes	3-90
List of IP Static Routes	3-90
Packet Filters	3-92
List of IP Packet Filters	3-92
Route Exports	3-95
List of Exports	3-95
IP over X.25	3-100
AppleTalk	3-101
Enabling the AppleTalk Protocol	3-101
Internet Packet Exchange (IPX)	3-102
IPX Service Advertisement Protocol (SAP) Filters	3-102
List of SAP Filters	3-103
IPX Router RIP Filters	3-104
List of IPX Router RIP Filters	3-105
IPX RIP Inbound Filters	3-106
List of IPX RIP Inbound Filters	3-106
IPX RIP Outbound Filters	3-107
List of IPX RIP Outbound Filters	3-108
Xerox Networking System (XNS)	3-109
XNS Inbound RIP Filters	3-109
List of XNS Inbound RIP Filters	3-110
XNS Outbound RIP Filters	3-111
List of XNS Outbound RIP Filters	3-111
XNS RIP Router Filters	3-112
List of XNS Router RIP Filters	3-113
List of XNS Static Routes	3-114
DECnet	3-115
DECnet Router Defaults	3-116
DECnet Packet Filters	3-119
List of DECnet Packet Filters	3-120

About this Chapter

This chapter provides information about the System Configuration parameters. (System Configuration is one of the initial configuration options present on the Configuration Main Menu. System Configuration sets the parameters that identify the IBM 6611 to the network.) This chapter is designed as a reference for Chapter 1 and Appendix A.

Each parameter contains the following information:

Parameter Name	Provides the name of the parameter.
Description	Provides the function of the parameter.
Required	Tells you whether the parameter must be configured to complete the configuration.
Dependencies	Tells you about any related parameters that can affect the way this parameter is configured.
Valid Values	Provides the range of values that can be used.
Default Value	Provides the preset value in the Configuration Program.

Source Route Bridging

Use the worksheet on page A-2.

Local and remote source route bridging are supported. Source route bridging is supported only for frames that begin and end on workstations that are attached to a ring. The source route bridging protocol on the IBM 6611 uses a proprietary bridge protocol data unit (BPDU).

AppleTalk, XNS, IPX, IP, DECnet, SNA, and NetBIOS protocols can be bridged. To send SNA and NetBIOS frames over the Token-Ring Network 16/4 Adapter, EIA 422/449 Serial Adapter, or V.35/V.36 Serial Adapter, bridging must be configured first.

Restrictions: When bridging has been defined for a token-ring port, all protocols that have not been configured to be routed are bridged automatically without further configuration. When bridging is not configured, packets of that protocol are discarded when the protocol has not been configured for routing.

Enable Source Route Bridging: This parameter enables or disables source route bridging of token-ring frames.

Required: No (Yes, if APPN is enabled)

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Bridge Number: This parameter uniquely identifies a bridge connecting two rings.

Required: Yes

Dependencies: This parameter is required when "Enable Source Route Bridging" is set to **Enable**.

Valid Values: 0 to 15

Default Value: None

Designated Ring Number: This parameter defines a set of token-ring ports that are treated as one virtual ring. The ring number must be unique within a token-ring network. The ring number is used in source route bridging just like a physical ring number. Therefore, it can appear as a route descriptor in the RIF information of source route bridge packets.

Required: Yes

Dependencies: This parameter is required when "Enable Source Route Bridging" is set to **Enable**.

Valid Values: X'001' to X'FFE'

Default Value: None

Spanning Tree Parameters

These parameters apply only to ports configured for spanning tree, when “Spanning Tree Mode” on page 6-6 is set to **automatic**.

Bridge Priority: This parameter is the priority component of the bridge identifier that is used to determine the root bridge for the spanning tree network.

Required: No

Dependencies: When “Spanning Tree Mode” on page 6-6 is set to **automatic**, this parameter applies only to ports configured for spanning tree.

Valid Values: X'0000' to X'FFFF'

Default Value: X'8000'

Hello Time: When this bridge is selected as the root bridge, this parameter specifies how often this bridge transmits configuration bridge protocol data units (BPDUs). BPDUs contain information about the topology of the spanning tree and reflect changes to the topology.

Required: No

Dependencies: When “Spanning Tree Mode” on page 6-6 is set to **automatic**, this parameter applies only to ports configured for spanning tree.

Valid Values: 1 to 10 seconds

Default Value: 2 seconds

Forward Delay Time: When this bridge is selected as the root bridge, the value of this parameter specifies how long active ports in all bridges remain in a *listening state*. When the forward delay time expires, ports in the listening state go into the *forwarding state*. State changes occur as a result of changes in the topology of the spanning tree, such as when an active bridge fails or is shut down.

In a source route bridge, spanning tree port states only affect spanning tree explorer (single route broadcast) frames. If a port is in the forwarding state, it forwards spanning tree explorer frames; otherwise the frames are not forwarded. Nonbroadcast and all routes explorer (all routes broadcast) frames may be forwarded by a port regardless of the port state.

Required: No

Dependencies: When “Spanning Tree Mode” on page 6-6 is set to **automatic**, this parameter applies only to ports configured for spanning tree.

Valid Values: 4 to 30 seconds

Default Value: 15 seconds

Maximum Age: When this bridge is selected as the root bridge, the value of this parameter specifies how long other active bridges are to store the configuration bridge protocol data units (BPDUs) they receive. If a BPDU reaches its maximum age limit without being replaced, the active bridges in the network discard it and assume that the root bridge has failed. A new root bridge is then selected.

Required: No

Dependencies: When “Spanning Tree Mode” on page 6-6 is set to **automatic**, this parameter applies only to ports configured for spanning tree.

Valid Values: 6 to 40 seconds

Default Value: 20 seconds

Port Filter Order

The parameters in this section enable you to define the order in which inbound and outbound filters should be applied on all IBM 6611 ports configured for source route bridging. The ordering of filters is optional and is done by filter type. The default order is:

1. Hop count filters
2. Source SAP filters
3. SNAP value filters
4. Ring number filters
5. MAC address filters
6. Sliding window filters.

You can improve the performance of the source route bridge by applying filters in the order in which they are most likely to be effective. The result is that the majority of unwanted traffic is discarded in the shortest amount of time, freeing buffer space to accommodate more traffic. For example, suppose you want to define the following filters:

- A SNAP value filter to deny all IP frames
- A MAC address filter to deny all frames from a specific MAC address.

In this scenario, IP frames represent the majority of the traffic that must be filtered out. By applying SNAP value filters first, you ensure that the largest percentage of unwanted traffic will be discarded in the shortest amount of time. MAC address filters, in this scenario, should be applied second because this filter type is expected to filter out a smaller percentage of traffic.

Source route bridge filters are defined and enabled on individual ports. The use of filters is optional. When configuring a port for source route bridging, you also can specify the order in which inbound and outbound filter types should be applied on that particular port. When filter ordering is specified on an individual port, the port settings override the settings of the parameters in this section.

Hop Count Filter: This parameter controls when the hop count filter type is to be applied on all IBM 6611 ports that support source route bridging. The hop count filter is applied only to inbound frames.

Source route bridge filter types are applied in a predefined order. That order is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: No

Dependencies: If you change the value of this parameter, the order of the other filter types must be changed accordingly. The value of this parameter cannot match the value specified for another filter type.

The order in which filter types are applied also can be configured on individual ports. The port parameter “Hop Count Filter” on page 6-16 determines the order in which inbound hop count filters are applied on a port. When configured, this port parameter overrides the value specified by this parameter. When this port parameter is not configured, the value of this parameter is used to determine when the hop count filter type is applied on a port.

Valid Values: 1 to 6, where 1 specifies that this filter type should be applied **first** on all source route bridging ports, and 6 specifies that this filter type should be applied **last**.

Default Value: 1

Source SAP Filter: This parameter controls when the source SAP filter type is to be applied on all IBM 6611 ports that support source route bridging. Source route bridge filter types are applied in a predefined order, and that order is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: No

Dependencies: If you change the value of this parameter, the order of the other filter types must be changed accordingly. The value of this parameter cannot match the value specified for another filter type.

The order in which filter types are applied also can be configured on individual ports. The port parameter “Source SAP Filter” on page 6-17 determines the order in which inbound source SAP filters are applied on a port. The port parameter “Source SAP Filter” on page 6-26 determines the order in which outbound source SAP filters are applied on a port. When configured, these port parameters override the value specified by this parameter. When these port parameters are not configured, the value of this parameter is used to determine when the source SAP filter type is applied on a port.

Valid Values: 1 to 6, where 1 specifies that this filter type should be applied **first** on all source route bridging ports, and 6 specifies that this filter type should be applied **last**.

Default Value: 2

SNAP Value Filter: This parameter controls when the SNAP value filter type is to be applied on all IBM 6611 ports that support source route bridging. Source route bridge filter types are applied in a predefined order, and that order is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: No

Dependencies: If you change the value of this parameter, the order of the other filter types must be changed accordingly. The value of this parameter cannot match the value specified for another filter type.

The order in which filter types are applied also can be configured on individual ports. The port parameter “SNAP Value Filter” on page 6-17 determines the order in which inbound SNAP value filters are applied on a port. The port parameter “SNAP Value Filter” on page 6-26 determines the order in which outbound SNAP value filters are applied on a port. When configured, these port parameters override the value specified by this parameter. When these port parameters are not

configured, the value of this parameter is used to determine when the SNAP value filter type is applied on a port.

Valid Values: 1 to 6, where 1 specifies that this filter type should be applied **first** on all source route bridging ports, and 6 specifies that this filter type should be applied **last**.

Default Value: 3

Ring Number Filter: This parameter controls when the ring number filter type is to be applied on all IBM 6611 ports that support source route bridging. Source route bridge filter types are applied in a predefined order, and that order is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: No

Dependencies: If you change the value of this parameter, the order of the other filter types must be changed accordingly. The value of this parameter cannot match the value specified for another filter type.

The order in which filter types are applied also can be configured on individual ports. The port parameter “Ring Number Filter” on page 6-17 determines the order in which inbound ring number filters are applied on a port. The port parameter “Ring Number Filter” on page 6-26 determines the order in which outbound ring number filters are applied on a port. When configured, these port parameters override the value specified by this parameter. When these port parameters are not configured, the value of this parameter is used to determine when the ring number filter type is applied on a port.

Valid Values: 1 to 6, where 1 specifies that this filter type should be applied **first** on all source route bridging ports, and 6 specifies that this filter type should be applied **last**.

Default Value: 4

MAC Address Filter: This parameter controls when the MAC address filter type is to be applied on all IBM 6611 ports that support source route bridging. Source route bridge filter types are applied in a predefined order, and that order is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: No

Dependencies: If you change the value of this parameter, the order of the other filter types must be changed accordingly. The value of this parameter cannot match the value specified for another filter type.

The order in which filter types are applied also can be configured on individual ports. The port parameter “MAC Address Filter” on page 6-17 determines the order in which inbound MAC address filters are applied on a port. The port parameter “MAC Address Filter” on page 6-27 determines the order in which outbound MAC address filters are applied on a port. When configured, these port parameters override the value specified by this parameter. When these port parameters are not configured, the value of this parameter is used to determine when the MAC address filter type is applied on a port.

Valid Values: 1 to 6, where 1 specifies that this filter type should be applied **first** on all source route bridging ports, and 6 specifies that this filter type should be applied **last**.

Default Value: 5

Sliding Window Filter: This parameter controls when the sliding window filter type is to be applied on all IBM 6611 ports that support source route bridging. Source route bridge filter types are applied in a predefined order, and that order is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: No

Dependencies: If you change the value of this parameter, the order of the other filter types must be changed accordingly. The value of this parameter cannot match the value specified for another filter type.

The order in which filter types are applied also can be configured on individual ports. The port parameter “Sliding Window Filter” on page 6-18 determines the order in which inbound sliding window filters are applied on a port. The port parameter “Sliding Window Filter” on page 6-27 determines the order in which outbound sliding window filters are applied on a port. When configured, these port parameters override the value specified by this parameter. When these port parameters are not configured, the value of this parameter is used to determine when the sliding window filter type is applied on a port.

Valid Values: 1 to 6, where 1 specifies that this filter type should be applied **first** on all source route bridging ports, and 6 specifies that this filter type should be applied **last**.

Default Value: 6

Transparent Bridging

Use the worksheet on page A-4.

The IBM 6611 supports Ethernet transparent bridging, as defined in the IEEE standard for Media Access Control Bridges (802.1D). The IBM 6611 also supports local and remote transparent bridging of all network protocols.

Note: The IBM 6611 does not provide support for source routing transparent bridging.

Local transparent bridging is the bridging of frames between Ethernet LANs directly attached to the same IBM 6611. Remote transparent bridging is the bridging of frames between Ethernet LANs that are attached to separate IBM 6611s. Remote transparent bridging is supported over a telecommunications link or frame relay network.

Each Ethernet LAN is attached to the IBM 6611 by means of an Ethernet Adapter. Transparent bridging needs to be configured at the system level and on each adapter port over which frames will be bridged. In addition, each IBM 6611 participating in remote bridging requires either an EIA 422/449 Serial Adapter or a V.35/V.36 Serial Adapter to communicate over a telecommunications link or frame relay network. Transparent bridging needs to be configured on each serial adapter port connected to a remote bridge.

Note: To perform remote transparent bridging, you must select either PPP (Point-to-Point Protocol) or Frame Relay as the frame encapsulation method for the serial adapter port.

Restrictions

- On the IBM 6611, the source and destination networks for transparent bridging must be Ethernet LANs.
- When an IBM 6611 acts as an intermediate bridge between two remote transparent bridges, the IBM 6611 must contain at least one enabled LAN adapter (Ethernet or Token-Ring Network 16/4) before the transparent bridge can be successfully started. The IBM 6611 requires a local MAC address to generate a bridge identifier for the transparent bridge. A LAN adapter is required in this case even if the IBM 6611 is not providing the local transparent bridging function.
- When transparent bridging has been defined on an Ethernet or serial adapter port, protocols that are not configured for routing are bridged automatically without further configuration. When a protocol is not configured for routing, and bridging is not configured, the IBM 6611 discards any packets it receives for that particular protocol.
- When defining transparent bridging on a serial adapter configured to support frame relay, you need to specify at least one data link connection identifier (DLCI) that will be used to transmit transparent bridge frames over the frame relay network.
- When adding an IBM 6611 to a transparent bridging network, the IBM 6611 should be connected to the network before the transparent bridging function is enabled. If an active bridge is dynamically connected to a network containing other bridges, network traffic may loop temporarily until the spanning tree detects the topology change.

The parameters in this section are configured once for the transparent bridging component of the IBM 6611.

Enable Transparent Bridging: This parameter enables or disables transparent bridging on the IBM 6611. When transparent bridging is enabled, protocols that are not configured for routing (on an Ethernet Adapter, EIA 422/449 Serial Adapter, or V.35/V.36 Serial Adapter) are bridged. This parameter must be set to **Enable** if data link switching is configured to forward NetBIOS and SNA frames on this port.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Form of MAC Addresses: This parameter specifies how the MAC addresses you enter are interpreted by the IBM 6611. Addresses can be in canonical form and non-canonical form.

In non-canonical form, the first bit transmitted is represented as the most significant bit. In canonical form, the first bit transmitted is represented as the least significant bit. For example, the following bit sequence:

0001 0011 0000 0000 0101 1010 0000 0000 0000 0000 0000 0001

is represented in non-canonical form as X'13 00 5A 00 00 01'. The same bit sequence, in canonical form, is represented as X'C8 00 5A 00 00 80'. Ethernet addresses are typically represented in canonical form.

Required: No

Dependencies: None

Valid Values: Canonical, Non-canonical

Default Value: Canonical

LLC Duplicate Address Check: This parameter indicates whether this transparent bridge participates in the IEEE 802.2 Duplicate Address Check protocol. Select **Forward** to instruct the bridge to forward frames that have identical source and destination addresses. Select **Filter** to instruct the bridge to discard all frames that have identical source and destination addresses.

Required: No

Dependencies: None

Valid Values: Forward, Filter

Default Value: Forward

Filtering Database Parameters

The following parameters are configured for the transparent bridge's filtering database.

Overflow Policy: This parameter specifies how the transparent bridge should handle a new entry for the filtering database if the database is full. Select **Learn** (the default) to instruct the bridge to discard an old entry in the database and replace it with the new entry. Select **Do not Learn** to instruct the bridge to discard the new entry, leaving the database unchanged. The filtering database can contain up to 4096 entries.

The bridge generates new entries for the filtering database by observing the source addresses of the frames it receives on each of its ports. Entries generated in this manner are called *dynamic entries*. The database associates the source address of the sending device with the port through which it can be reached. In this way, the bridge "learns" about the location of specific devices in the network. Dynamic entries in the database are aged and discarded to accommodate changes in the logical topology of the network (see "Aging Time").

Required: No

Dependencies: None

Valid Values: Learn, Do not Learn

Default Value: Learn

Aging Time: This parameter specifies the number of seconds that a dynamic entry can remain in the filtering database without the transparent bridge observing any activity from that address. When the age of an entry equals the aging time, the bridge deletes the entry from the filtering database.

The bridge generates dynamic entries for the filtering database by observing the source addresses of the frames it receives on each of its ports. The database associates the source address of the sending device with the port through which it can be reached. In this way, the bridge "learns" about the location of specific devices in the network.

Required: No

Dependencies: None

Valid Values: 10 to 1 000 000 seconds

Default Value: 300 seconds

Static Destination Address Filters

The filtering database for the IBM 6611 can contain up to 4096 static destination address filters. The IEEE 802.1D standard for MAC bridges defines 16 default static destination address filters, which are automatically included in the filtering database. You can define an additional 4080 filters.

The 16 default filters include the bridge group address X'01 80 C2 00 00 00' and reserved MAC addresses X'01 80 C2 00 00 01' through X'01 80 C2 00 00 0F' (in canonical form). If a frame is received with one of these destination MAC addresses, the frame is not forwarded by the transparent bridge.

Because static destination address filters are processed before individual port filters, these filters offer a performance advantage. However, because static destination address filters apply to all transparent bridge ports, these filters should be used only if a destination address needs to be filtered on all ports for both inbound and outbound frames.

Static Destination MAC Address: This parameter specifies a static destination MAC address that is placed in the filtering database. The bridge discards (filters) any frame it receives on a bridge port with the specified destination address.

This address is **static** because it remains in the filtering database until you remove or change it. Each static address you define reduces the amount of space available in the filtering database for dynamic entries.

This parameter affects only frames handled by the transparent bridge. Routed frames are not affected by this parameter.

Required: No

Dependencies: None

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

Port Filter Order

The parameters in this section enable you to define the order in which inbound and outbound filters should be applied on all IBM 6611 ports configured for transparent bridging. Defining the order of filters is optional and is done by filter type. The default order is:

1. Source SAP filters
2. Ethernet Type filters
3. MAC address filters
4. Sliding window filters.

You can improve the performance of the transparent bridge by applying filters in the order in which they are most likely to be effective. The result is that the majority of unwanted traffic is discarded in the shortest amount of time, freeing buffer space to accommodate more traffic. For example, suppose you want to define the following port filters:

- An Ethernet Type filter to deny all IP frames
- A MAC address filter to deny all frames from a specific MAC address.

In this scenario, IP frames represent the majority of the traffic that must be filtered out. By applying Ethernet Type filters first, you ensure that the largest percentage of unwanted traffic will be discarded in the shortest amount of time. MAC address filters, in this scenario, should be applied second because this filter type is expected to filter out a smaller percentage of traffic.

Transparent bridge filters are defined and enabled on individual ports. The use of filters is optional. When configuring a port for transparent bridging, you can specify the order in which inbound and outbound filter types should be applied on that particular port. When filter ordering is specified on an individual port, the port settings override the settings of the parameters in this section.

Source SAP Filter: This parameter controls when the source SAP filter type is to be applied on all IBM 6611 ports that support transparent bridging. Transparent bridge filter types are applied in a predefined order, and that order is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: No

Dependencies: If you change the value of this parameter, the order of the other filter types must be changed accordingly. The value of this parameter cannot match the value specified for another filter type.

The order in which filter types are applied also can be configured on individual ports. The port parameter “Source SAP Filter” on page 6-40 determines the order in which inbound source SAP filters are applied on a port. The port parameter “Source SAP Filter” on page 6-47 determines the order in which outbound source SAP filters are applied on a port. When configured, these port parameters override the value specified by this parameter. When these port parameters are not configured, the value of this parameter is used to determine when the source SAP filter type is applied on a port.

Valid Values: 1 to 4, where 1 specifies that this filter type should be applied **first** on all transparent bridge ports, and 4 specifies that this filter type should be applied **last**.

Default Value: 1

Ethernet Type Filter: This parameter controls when Ethernet Type filters are to be applied on all IBM 6611 ports that support transparent bridging. The Ethernet Type filter is applied to the contents of the Type field within an Ethernet frame. The Type field identifies the type of data encapsulated within an Ethernet Version 2 frame or IEEE 802.3 frame with a SNAP header.

Transparent bridge filter types are applied in a predefined order, and that order is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: No

Dependencies: If you change the value of this parameter, the order of the other filter types must be changed accordingly. The value of this parameter cannot match the value specified for another filter type.

The order in which filter types are applied also can be configured on individual ports. The port parameter “Ethernet Type Filter” on page 6-40 determines the order in which inbound Ethernet type filters are applied on a port. The port parameter “Ethernet Type Filter” on page 6-48 determines the order in which outbound Ethernet type filters are applied on a port. When configured, these port parameters override the value specified by this parameter. When these port parameters are not configured, the value of this parameter is used to determine when Ethernet type filters are applied on a port.

Valid Values: 1 to 4, where 1 specifies that this filter type should be applied **first** on all transparent bridge ports, and 4 specifies that this filter type should be applied **last**.

Default Value: 2

MAC Address Filter: This parameter controls when the MAC address filter type is to be applied on all IBM 6611 ports that support transparent bridging. Transparent bridge filter types are applied in a predefined order, and that order is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: No

Dependencies: If you change the value of this parameter, the order of the other filter types must be changed accordingly. The value of this parameter cannot match the value specified for another filter type.

The order in which filter types are applied also can be configured on individual ports. The port parameter “MAC Address Filter” on page 6-40 determines the order in which inbound MAC address filters are applied on a port. The port parameter “MAC Address Filter” on page 6-48 determines the order in which outbound MAC address filters are applied on a port. When configured, these port parameters override the value specified by this parameter. When these port parameters are not configured, the value of this parameter is used to determine when the MAC address filter type is applied on a port.

Valid Values: 1 to 4, where 1 specifies that this filter type should be applied **first** on all transparent bridge ports, and 4 specifies that this filter type should be applied **last**.

Default Value: 3

Sliding Window Filter: This parameter controls when the sliding window filter type is to be applied on all IBM 6611 ports that support transparent bridging. Transparent bridge filter types are applied in a predefined order, and that order is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: No

Dependencies: If you change the value of this parameter, the order of the other filter types must be changed accordingly. The value of this parameter cannot match the value specified for another filter type.

The order in which filter types are applied also can be configured on individual ports. The port parameter “Sliding Window Filter” on page 6-40 determines the order in which inbound sliding window filters are applied on a port. The port parameter “Sliding Window Filter” on page 6-48 determines the order in which outbound sliding window filters are applied on a port. When configured, these port parameters override the value specified by this parameter. When these port parameters are not configured, the value of this parameter is used to determine when the sliding window filter type is applied on a port.

Valid Values: 1 to 4, where 1 specifies that this filter type should be applied **first** on all transparent bridge ports, and 4 specifies that this filter type should be applied **last**.

Default Value: 4

Spanning Tree Parameters

The following parameters define this transparent bridge's contribution to the spanning tree for the bridged network.

Bridge Priority: This parameter specifies the priority of this transparent bridge. When this bridge is activated by the network administrator, its priority value is compared to the priority values of other active bridges in the network. The bridge with the highest priority becomes the root bridge of the spanning tree.

If the highest priority value in the network is shared by two or more bridges, the bridges compare Ethernet port MAC addresses (one port on each bridge is selected for this purpose). The bridge with the lowest value MAC address becomes the root bridge.

Required: No

Dependencies: None

Valid Values: X'0000' to X'FFFF', where X'0000' is the **highest** priority value and X'FFFF' is the **lowest** priority value

Default Value: X'8000'

Hello Time: When this bridge is selected as the root bridge, this parameter specifies how often this bridge transmits configuration bridge protocol data units (BPDUs). BPDUs contain information about the topology of the spanning tree and reflect changes to the topology.

Required: No

Dependencies: The setting of this parameter may affect the setting of the parameter "Max Age" on page 3-17. The IEEE standard for Media Access Control Bridges (802.1D) recommends that the relationship between the parameters be defined using the formula

$$\text{Max age} \geq (\text{Hello time} + 1) \times 2$$

The Configuration Program will enforce the relationship stated in the formula and adjust the Max age parameter value, as needed, to accommodate changes in the Hello time value.

Valid Values: 1 to 10 seconds

Default Value: 2 seconds

Forward Delay: When this bridge is selected as the root bridge, the value of this parameter specifies how long ports in all bridges remain in either a *listening state* or *learning state*. When the forward delay time expires, ports in the listening state go into the learning state and ports in the learning state go into the forwarding state. State changes occur as a result of changes in the topology of the spanning tree, such as when an active bridge fails or is shut down.

In order to keep the information in the filtering database current, the value of this parameter also is used as the value of the Aging time parameter for a short period after a topology change occurs.

Required: No

Dependencies: The setting of this parameter may be affected by the setting of the parameter "Max Age" on page 3-17. The IEEE standard for Media Access Control Bridges (802.1D) recommends that the relationship between the parameters be defined using the formula

$$2 \times (\text{Forward delay} - 1) \geq \text{Max age}$$

The Configuration Program will enforce the relationship stated in the formula and adjust the Forward delay value, as needed, to accommodate the Max age value.

Valid Values: 4 to 30 seconds

Default Value: 15 seconds

Max Age: When this bridge is selected as the root bridge, the value of this parameter specifies how long other active bridges are to store the configuration bridge protocol data units (BPDUs) they receive. If a BPDU reaches its maximum age limit without being replaced, the active bridges in the network discard it and assume that the root bridge has failed. A new root bridge is then selected.

Required: No

Dependencies: The setting of this parameter may be affected by the setting of the parameter "Hello Time" on page 3-16. In addition, the setting of this parameter may affect the setting of the parameter "Forward Delay" on page 3-16. The IEEE standard for Media Access Control Bridges (802.1D) recommends that the relationships between these parameters be defined using the formulas

$$\text{Max age} \geq (\text{Hello time} + 1) \times 2$$

$$2 \times (\text{Forward delay time} - 1) \geq \text{Max age}$$

The Configuration Program will enforce the relationships stated in the formulas and:

- Adjust the setting of Max age to accommodate the Hello time value.
- Adjust the Forward delay value to accommodate the setting for Max age.

Valid Values: 6 to 40 seconds

Default Value: 20 seconds

Data Link Switching

Use the worksheet on page A-2.

Data link switching enables two SNA devices or two NetBIOS stations to communicate with each other across an intervening IP network. The end station must rely on an IBM 6611 attached to its network to provide a connection across the IP network to the remote station. Data link switching uses source route bridging from an end station to the IBM 6611 that provides the connection. Therefore, to the source station, the destination station appears to be ring attached.

Notes:

1. In the Configuration Program, data link switching is configured only by using System Configuration.
2. Data Link Switching must be configured in order to run the APPN protocol.

You must configure the following functions when you want this IBM 6611 to provide data link switching function:

Table 3-1. SNA and NetBIOS Configuration Requirements

Protocol	Adapter	Configuration Requirements
NetBIOS	Token-Ring, Ethernet, EIA 422/449 Serial Adapter, or V.35/V.36 Serial Adapter	Data link switching must be configured (NetBIOS enabled). NetBIOS and source route bridging must be configured on a port for Token-Ring Network 16/4 Adapter, EIA 422/449 Serial Adapter, V.35/V.36 Serial Adapter, or transparent bridging on Ethernet. At least one data link switching partner must be defined and IP must be configured on some port.
SNA	Token-Ring or Ethernet	Token-ring ports must be configured for source route bridging and SNA. Ethernet ports must be configured for transparent bridging and SNA. Data link switching must be configured (SNA enabled). SNA must be configured on a token-ring port or Ethernet port. If there is no SDLC Adapter installed, then at least one data link switching partner must be defined and IP must be configured on some port. If there is an SDLC Adapter installed, then no data link switching partners need to be defined and IP does not have to be configured on some port.
SNA NetBIOS	EIA 422/449 Serial Adapter or V.35/V.36 Serial Adapter	Serial ports must be configured for SNA, transparent bridging, and source route bridging. If there is no SDLC Adapter installed, then at least one data link switching partner must be defined and IP must be configured on some port. If there is an SDLC Adapter installed, then no data link switching partners need to be defined and IP does not have to be configured on some port.
SNA	SDLC	SDLC Adapter parameters must be configured. The SDLC parameters start on page 5-22. Each SNA station must be configured. The SNA station parameters start on page 5-25. data link switching must be enabled (SNA enabled). There are no SNA parameters for an SDLC port.

Restrictions

- See Table 3-1.
- When you configure IPX and XNS, you cannot use the SAPs, which are X'E0' for IPX and X'80' for XNS, to route data link switching traffic.

Configuring Data Link Switching

The following information should be applied if you want to configure an IBM 6611 for data link switching. The IBM 6611 must:

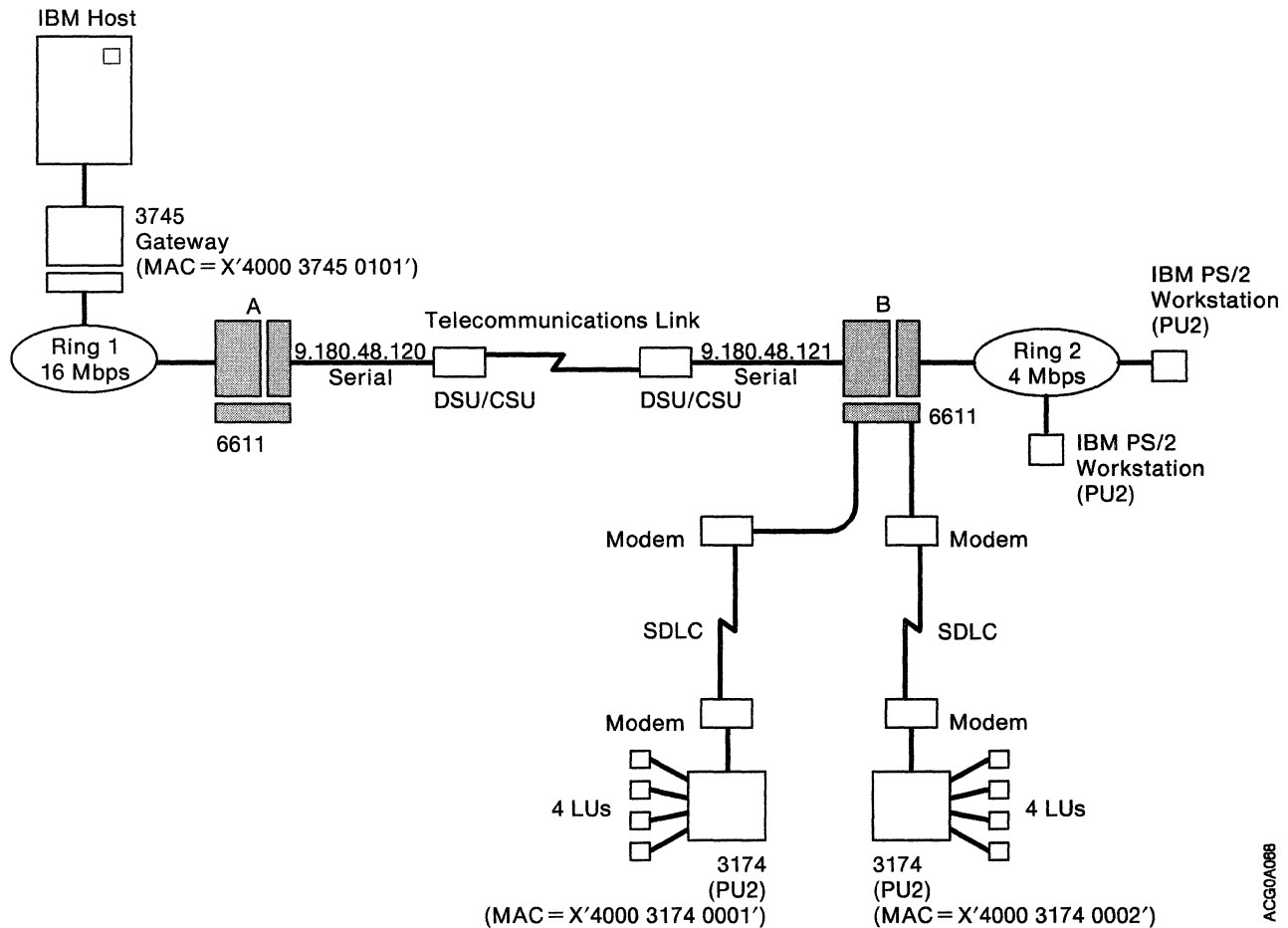
- Contain an adapter that is configured for data link switching: for example, an SDLC Adapter, Ethernet Adapter, or Token-Ring Network 16/4 Adapter. If you are using a Token-Ring Network 16/4 Adapter, you must configure bridging. If the IBM 6611 contains multiple Token-Ring Network 16/4 Adapters that are configured for bridging, any one of those adapters can be configured for data link switching.
- Contain at least one port that is configured for IP and is attached to the network over which this IBM 6611 can communicate with its data link switching partners. That port can be any IBM 6611 adapter that supports IP. If the IBM 6611 contains multiple ports that are configured for IP and can be used to communicate with the partners, the IBM 6611 selects one of the IP ports through which to forward the IP datagrams.

Figure 3-1 on page 3-20 shows a sample network in which the IBM 6611s are configured for data link switching. The 3745 is token-ring attached. The 3174s use SNA to communicate to the IBM host via the 3745 gateway. The token-ring MAC address of the 3745 should be configured as the station destination address on the 3174s when they are communicating through the 3745 gateway.

6611 A is connected to Ring 1 via a Token-Ring Network 16/4 Adapter and to the telecommunications link via an EIA 422/449 Serial Adapter.

6611 B is connected to Ring 2 via a Token-Ring Network 16/4 Adapter and to the telecommunications link via an EIA 422/449 Serial Adapter. 6611 B is link attached to each 3174 via an SDLC Adapter.

In each case, the EIA 422/449 Serial Adapters are connected to a DSU/CSU and the SDLC Adapters are connected to a modem.



ACG0A088

Figure 3-1. Sample Network Using Data Link Switching

In this scenario, the following configuration is required for 6611 A:

- Port-Level

1. Configure the Token-Ring Network 16/4 Adapter port.

- a. Add the Token-Ring Network 16/4 Adapter.

- 1) Select an adapter slot by clicking on the numbered push button that corresponds to the slot that you want to configure. (You cannot select the physical slot.)
 - 2) A pop-up window appears that allows you to add an adapter.
 - 3) When you select **Add**, a pop-up window appears. Click on the Token-Ring Network 16/4 Adapter.
 - 4) To configure the port, select the port by clicking on the adapter port on the window.

- b. Select the Physical Interface push button.

- 1) Enable the interface.
 - 2) Set the token-ring data rate to 16 Mbps.
 - 3) Configuring a locally administered address is optional.

- c. Enable SR Bridge.

- d. Select the SR Bridge push button.

- Configure the number for Ring 1. In this scenario, the ring number is 001. The system administrator can determine the correct ring number for your network.
 - e. In the SR Bridge Required area, enable SNA.
- 2. Configure the EIA 422/449 Serial Adapter port 1.
 - a. Add the EIA 422/449 Serial Adapter.
 - 1) Select an adapter slot by clicking on the numbered push button that corresponds to the slot that you want to configure. (You cannot select the physical slot.)
 - 2) A pop-up window appears that allows you to add an adapter.
 - 3) When you select Add, a pop-up window appears. Click on the EIA 422/449 Serial Adapter.
 - 4) To configure the port, select the port by clicking on the adapter port on the window.
 - b. Select PPP from the pop-up window.
 - c. Enable IP.
 - d. Select the IP push button.
 - 1) Enter a unique IP address. In this scenario, the IP address is 9.180.48.120. Configuring a subnet mask is optional. An example value of a subnet mask is 255.255.252.0.
 - 2) Define the destination IP address. In this scenario, the destination IP address selected is 9.180.48.121 (the IP address of the EIA 422/449 Serial Adapter port on 6611 B).

- System Configuration

- 1. Configure source route bridging
 - a. In the Bridging area of the window, enable SR Bridge.
 - b. Select the SR bridge push button.
 - c. Configure a bridge number. The bridge number in this scenario is 1.
- 2. Configure data link switching.
 - a. In the data link switching area of the window, enable the forwarding of SNA traffic.
 - b. Select the data link switching push button.
 - 1) Enter the virtual ring segment number. The virtual segment number must be the same for the data link switching partners, but unique through the entire network. An example of a virtual segment ring number is FAB.
 - 2) Select a default data link switching IP address from the list of available IP addresses for 6611 A. 6611 B will use this IP address to send traffic to 6611 A.
 - 3) Select the data link switching partners push button.
 - 4) Enter the IP address of the remote IBM 6611. It can be the IP address of an EIA 422/449 Serial Adapter, Token-Ring Network 16/4 Adapter, Ethernet Adapter, or X.25 Adapter. In this scenario, the IP address is 9.180.48.121 (the IP address of the EIA 422/449 Serial Adapter port on 6611 B).

In this scenario, the following configuration is required for IBM 6611 B:

- Port-Level

1. Configure a Token-Ring Network 16/4 Adapter port.

- a. Add a Token-Ring Network 16/4 Adapter.

- 1) Select an adapter slot by clicking on the numbered push button that corresponds to the slot that you want to configure. (You cannot select the physical slot.)
- 2) A pop-up window appears that allows you to add an adapter.
- 3) When you select **Add**, a pop-up window appears. Click on the Token-Ring Network 16/4 Adapter.
- 4) To configure the port, select the port by clicking on the adapter port on the screen.

- b. Select the Physical Interface push button.

- 1) Enable the interface.
- 2) Set the token-ring data rate to 4 Mbps.
- 3) Configuring a locally administered address is optional.

- c. Enable SR Bridge.

- d. Select the SR Bridge push button.

- Configure the ring number for Ring 2. In this scenario the ring number is 002. The system administrator can determine the correct ring number for your network.

- e. In the SR Bridge Required window, enable SNA.

2. Configure the EIA 422/449 Serial Adapter port 1.

- a. Add an EIA 422/449 Serial Adapter.

- 1) Select an adapter slot by clicking on the numbered push button that corresponds to the slot that you want to configure. (You cannot select the physical slot.)
- 2) A pop-up window appears that allows you to add an adapter.
- 3) When you select **Add**, a pop-up window appears. Click on the EIA 422/449 Serial Adapter.
- 4) To configure the port, select the port by clicking on the adapter port on the window.

- b. Select PPP from the pop-up window.

- c. Enable IP.

- d. Select the IP push button.

- 1) Enter a unique IP address. In this scenario, the IP address is 9.180.48.121. The subnet mask is optional. An example value of a subnet mask is 255.255.252.0.
- 2) Define the destination IP address. In this scenario, the destination IP address is 9.180.48.120.

Note: This completes the minimal configuration that is required for a PS/2 to communicate to a 3745 using an IBM 6611 network. Ask your system administrator for more information about configuring a PS/2.

3. Configure the SDLC Adapter Port 0.

a. Add an SDLC Adapter.

- 1) Select an adapter slot by clicking on the numbered push button that corresponds to the slot that you want to configure. (You cannot select the physical slot.)
- 2) A pop-up window appears that allows you to add an adapter.
- 3) When you select Add, a pop-up window appears. Click on the SDLC Adapter.
- 4) To configure the port, select the port by clicking on the adapter port on the window.

b. Select EIA 232-D on the pop-up window.

c. Select the Physical Interface push button.

- Verify that serial encoding, request to send, data rate select, and data terminal ready match the 3174 configuration. In this scenario, the defaults were used. The defaults are usually correct.

d. Select the SNA Stations push button.

- 1) Press the **Add** push button.
- 2) Enter a Station address, for example X'C1'.
- 3) Enter a Station token ring source address, for example X'4000 3174 0001'.
- 4) Enter a Station token-ring source SAP. In this scenario, this value must match the station token-ring destination SAP of the 3745 which is X'04'.
- 5) Enter the Station token-ring destination address, which is the 3745 gateway in this scenario. The value is X'4000 3745 0101'.
- 6) Enter the Station token-ring destination SAP, for example X'04'. In this scenario, the value must match the station token-ring source SAP of the 3745.
- 7) Enter the station XID value. This value must match IDBLK and IDNUM in VTAM on the host switched net member. In this scenario, the value is X'0170 0045'.
- 8) Press **Apply**. Additional SNA stations can be added. Each SNA station must have a unique station address, station token-ring source address, and station XID value.

Note: You can repeat these steps to configure other SDLC Adapters. In this scenario, two SDLC Adapter ports are configured.

4. Configure the SDLC Adapter Port 1.

a. Add an SDLC Adapter.

- 1) Select an adapter slot by clicking on the numbered push button that corresponds to the slot that you want to configure. (You cannot select the physical slot.)
- 2) A pop-up window appears that allows you to add an adapter.
- 3) When you select Add, a pop-up window appears. Click on the SDLC Adapter.

- 4) To configure the port, select the port by clicking on the adapter port on the window.
 - b. Select EIA 232-D on the pop-up window.
 - c. Select the Physical Interface push button.
 - Verify that serial encoding, request to send, data rate select, and data terminal ready match the 3174 configuration. In this scenario, the defaults were used. The defaults are usually correct.
 - d. Select the SNA Stations push button.
 - 1) Press the **Add** push button.
 - 2) Enter a Station address, for example X'C2'.
 - 3) Enter a Station token-ring source address, for example X'4000 3174 0002'.
 - 4) Enter a Station token-ring source SAP. In this scenario, this value must match the station token-ring destination SAP for the 3745 which is X'04'.
 - 5) Enter the Station token-ring destination address, which is the 3745 gateway in this scenario. The value is X'4000 3745 0101'.
 - 6) Enter the Station token-ring destination SAP, for example X'04'. In this scenario, the value must match the station token-ring source SAP of the 3745.
 - 7) Enter the station XID value. This value must match IDBLK and IDNUM in VTAM on the host switched net member. In this scenario, the value is X'0170 0046'.
 - 8) Press **Apply**. Additional SNA stations can be added. Each SNA station must have a unique station address, station token-ring source address, and station XID value.
- System Configuration
 1. Configure source route bridging.
 - a. In the Bridging area of the window, enable SR Bridge.
 - b. Select the SR Bridge push button.
 - Configure a bridge number. The bridge number in this scenario is 1.
 2. Configure data link switching.
 - a. In the data link switching area, enable the forwarding of SNA traffic.
 - b. Select the data link switching push button.
 - 1) Enter the virtual ring segment number. The virtual segment ring number must be the same for the data link switching partners, but unique through the entire network. An example virtual segment ring number is FAC.
 - 2) Select a default data link switching IP address from the list of available IP addresses for 6611 B. 6611 A will use this IP address to send traffic to 6611 B.
 - 3) Select the data link switching partners push button.
 - Enter the IP address of the remote IBM 6611. It can be the IP address of an EIA 422/449 Serial Adapter, Token-Ring Network

16/4 Adapter, Ethernet Adapter, or X.25 Adapter. In this scenario, the IP address is 9.180.48.120 (the IP address of the EIA 422/449 Serial Adapter port on 6611 A).

Enable Protocols Forwarded by Data Link Switching

Enable Forwarding of SNA Traffic: This parameter enables or disables the forwarding of SNA frames.

Required: No (Yes for APPN)

Dependencies: This parameter must be set to **Enable** to forward SNA traffic.

Valid Values: Enable, Disable

Default Value: Disable

Enable NetBIOS Frame Forwarding: This parameter enables or disables the forwarding of NetBIOS frames.

Required: No

Dependencies: This parameter must be set to **Enable** to perform NetBIOS frame forwarding.

Valid Values: Enable, Disable

Default Value: Disable

Data Link Switching Specific Parameters

Virtual Ring Segment Number: This parameter specifies a token-ring network segment number that is used in all frames passed to or from the IBM 6611 using data link switching. The virtual ring segment number must be a unique number through the entire network where the IBM 6611s reside. This value is assigned to the segment number placed in the token-ring routing information (RI) field to address frames to the data link switching function.

Required: No

Dependencies: The value of this parameter must be the same in all IBM 6611s attached to the same LAN segment or extended LAN segment.

Valid Values: X'0' to X'FFF'

Default Value: None (this field is blank)

Destination Cache Timeout: This parameter defines the length of time that this IBM 6611 considers using the information described by the IBM 6611 to forward frames to a particular MAC address or NetBIOS name.

Required: No

Dependencies: None

Valid Values: 1 to 20 minutes

Default Value: 8 minutes

Default Data Link Switching IP Address for this IBM 6611: This parameter defines the IP address that data link switching partners will use when sending SNA/NetBIOS frames to this IBM 6611 across an IP network.

Required: Yes

Dependencies: When this parameter is configured, this IP address must be configured on some interface on this IBM 6611.

Valid Values: A valid IP address

Default Value: None

Accept Connections Only from Specific IBM 6611s: This parameter controls whether this IBM 6611 accepts requests to establish a data link switching connection with other IBM 6611s that were configured for data link switching in "IP Address of Remote IBM 6611."

Required: No

Dependencies: When this parameter is set to **Accept**, the IBM 6611 accepts connections only from the partner routers specified in "List of Data Link Switching Partners." When this parameter is set to **Do not accept**, the IBM 6611 accepts connections from any IBM 6611 configured for data link switching in the network.

Valid Values: Enable, Disable

Default Value: Disable

List of Data Link Switching Partners

IP Address of Remote IBM 6611: This parameter defines the IP address of another IBM 6611 configured for data link switching with which this IBM 6611 can exchange SNA or NetBIOS traffic. This parameter is configured for each IBM 6611 to which this IBM 6611 can connect using data link switching.

Required: Yes

Dependencies: IP must be configured to use data link switching. This parameter is required to define the participating data link switching routers.

Valid Values: A valid IP address

Default Value: None

Systems Network Architecture (SNA)

Use the worksheet on page A-22.

List of SNA Default Destinations

The following parameters define the remote IBM 6611s that are used to search for the SNA end stations. This information limits the WAN search for a destination IBM 6611. If one or more IBM 6611s are listed in the table, the origin IBM 6611 directs its search only to the specified IBM 6611s rather than broadcast to all participating remote IBM 6611s. A single remote IBM 6611 may be the destination for multiple SNA end stations, and a single SNA end station may have multiple remote IBM 6611s as its destination.

IP Address of Destination Router: This parameter indicates a default router to be used to reach the destination name configured in "Destination MAC Address."

Required: Yes

Dependencies: This parameter is required to define the SNA default destinations.

Valid Values: Any router address configured in "Source Address" on page 3-28.

Default Value: None

Destination MAC Address: This parameter defines a token-ring destination MAC address for a default destination.

Required: Yes

Dependencies: This parameter is required when defining a destination.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

SNA Frame Filters

SNA allows the user to define a set of filters which are applied to frames transported using data link switching. Each filter is composed of a source name and destination name. The filter compares the source name and destination name of each SNA explorer frame with the configured list. *Explorer frames* are frames that are used to resolve a logical name to a MAC address. The purpose of filtering is to allow or disallow connection establishment between SNA stations. Filters are not applied to data frames sent after a connection is established. Unlike bridge filtering, data link switching filtering does not cause a performance impact.

Source Frame Filters

The following parameters configure the type of SNA source frame filters. These parameters are not required unless you want to configure SNA source frame filters. A maximum of 100 filters can be configured.

Status of All Defined SNA Source Frame Filters: The parameter enables or disables all SNA source frame filters configured. When SNA source frame filters are not defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Source Frame Filter Type: This parameter defines the type of SNA source frame filter you want for this port: a deny or a permit filter. The value you configure for this parameter applies to all of the SNA source frame filters that you configure.

Select **Deny** when you want all of the SNA source frame filters to block SNA source frames that contain a destination address and a source address that match addresses configured for "Source Address" and "Destination Address" on page 3-29. The filters do not pass those SNA source frames to the data link switching function.

Select **Permit** when you want all of the SNA source frame filters to pass SNA source frames that contain a destination address and a source address that match addresses configured for "Source Address" and "Destination Address" on page 3-29. The filter passes those SNA source frames to the data link switching function.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

List of SNA Source Frame Filters

The following parameters are configured for each SNA source frame filter that is defined. These parameters are not required unless you want to configure a list of SNA source frame filters. A maximum of 100 filters can be defined.

Filter ID: This parameter provides a unique identifier of this filter.

Required: Yes

Dependencies: This parameter must be configured for each SNA source frame filter. This parameter is required to define SNA source frame filters.

Valid Values: 1 to 100

Default Value: None

Source Address: This parameter defines the source MAC address that matches frames to which this filter is applied.

Required: Yes

Dependencies: This parameter must be configured for each SNA source frame filter. This parameter is required to define SNA source frame filters.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

Source Address Mask: This parameter contains the SNA source address mask that indicates which bits of the source address configured for “Source Address” to consider significant when using the filter. The mask is interpreted as follows: for every bit equal to one in the mask, the same bit in the address is considered significant.

Required: No

Dependencies: This parameter is configured for each SNA source frame filter.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: X'FFFF FFFF FFFF'

Destination Address: This parameter specifies the destination address that matches the packets to which this filter is applied.

Required: No

Dependencies: This parameter is configured for each SNA source frame filter. This parameter and “Destination Address Mask” are configured together to define the range of destination addresses to filter.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

Destination Address Mask: This parameter contains the destination address mask that indicates which bits of the destination address configured in “Destination Address” are considered significant when using the filter. This means that all networks are valid. The mask is interpreted as follows: for every bit equal to one in the mask, the same bit in the MAC address is considered significant.

Required: No

Dependencies: This parameter is configured for each SNA destination frame filter. This parameter and “Destination Address” are configured together to define the range of destination addresses to filter.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: X'FFFF FFFF FFFF'

Destination Frame Filters

These parameters configure the type of SNA destination frame filters. These parameters are not required. A maximum of 100 filters can be defined.

Status of All Defined SNA Destination Frame Filters: This parameter enables or disables the forwarding of SNA frames on this port with SAP values equal to one of the values configured in “SAP Value” on page 6-49. If “Enable SNA Frame Forwarding on This Port” on page 6-49 is set to **Disable**, the forwarding of SNA frames on this port is stopped, but the configuration information is retained.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Destination Frame Filter Type: When this parameter is set to **Permit**, all filters configured for SNA permit frames to be forwarded when they are valid values for source and destination addresses. When this parameter is set to **Deny**, all filters configured for SNA deny frames to be forwarded when they are valid values for source and destination addresses.

Required: No

Dependencies: This parameter is configured once for all filters. All filters must be **Deny** or **Permit**.

Valid Values: Deny, Permit

Default Value: Deny

List of Destination Frame Filters

Filter ID: This parameter provides a unique identifier for this filter.

Required: Yes

Dependencies: This parameter is configured for each SNA destination frame filter. This parameter is required to define destination frame filters.

Valid Values: 1 to 100

Default Value: None

Source Address: This parameter defines the source SNA address that matches frames to which this filter is applied.

Required: Yes

Dependencies: This parameter is required to define destination frame filters. It is configured for each SNA destination frame filter and is displayed in the list of destination frame filters. This parameter and "Source Address Mask" define the range of source addresses to filter.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

Source Address Mask: This parameter contains the SNA source address mask that indicates which bits of the source address configured for "Source Address" are considered significant when the filter is applied. The mask is interpreted as follows: for every bit equal to one in the mask, the same bit in the address is considered significant.

Required: No

Dependencies: This parameter is configured for each SNA destination frame filter and is displayed in the list of destination frame filters. This parameter and "Source Address" define the range of source addresses to filter.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: X'FFFF FFFF FFFF'

Destination Address: This parameter specifies the destination address that matches frames to which this filter is applied.

Required: No

Dependencies: This parameter is configured for each SNA destination frame filter and is displayed in the list of destination frame filters.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

Destination Address Mask: This parameter contains the destination address mask that indicates which bits of the destination address configured for “Destination Address” are considered significant when the filter is applied. The mask is interpreted as follows: for every bit equal to 1 in the mask, the bit at the same position in the destination address is considered significant. When the default mask of all zeros is used, bits in the destination address are not considered significant. This means that all networks are valid.

Required: No

Dependencies: This parameter is configured for each SNA destination frame filter and is displayed in the list of destination frame filters.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: X'FFFF FFFF FFFF'

Advanced Peer-to-Peer Networking

Note: The Advanced Peer-to-Peer Networking function described in this document will be available as part of Version 1 Release 1.2 of the IBM Multiprotocol Network Program.

Advanced Peer-to-Peer Networking* (APPN*) is an enhancement to IBM's SNA architecture and allows nodes to communicate as peers without requiring the services of an SNA host computer. APPN nodes are classified as type 2.1 (T2.1) nodes and extend the capabilities of T2.1 low-entry networking (LEN) nodes. Like LEN nodes, each APPN node contains a *control point* (CP) that is responsible for managing the resources of the node. Unlike LEN nodes, APPN nodes can share information about resources through CP-CP sessions, reducing the need to define the location of resources in the network.

The APPN architecture defines two types of APPN nodes: *network nodes* and *end nodes*. Network nodes provide directory, route selection, and management services for attached end nodes. End nodes provide limited directory, route selection, and management services for logical units (LUs) associated with the end node.

The IBM 6611 functions as a network node within an APPN network. As a network node, the IBM 6611 can provide services to attached APPN end nodes and act as an intermediate node that routes data between adjacent network nodes. The IBM 6611 network node also supports connections to LEN end nodes. Such connections can serve as entry points into an SNA subarea network.

For more information about how APPN is implemented on the IBM 6611, refer to the *IBM 6611 Network Processor Introduction and Planning Guide*.

Configuring an IBM 6611 Network Node

APPN is not configured on individual adapters, but supports definitions for:

- Data link switching (for SNA) on the Token-Ring Network 16/4 Adapter and the Ethernet Adapter
- IP on all 6611 adapters.

Note: An APPN node on an Ethernet LAN cannot have a CP-CP session with a locally-attached IBM 6611 network node. However, the APPN node can use the data link switching function on the locally-attached IBM 6611 to communicate with a remote IBM 6611 network node across a wide area network (WAN).

Data link switching must be configured on the IBM 6611 in order to run the APPN protocol. To enable APPN to communicate across a WAN, you need to define both data link switching and IP connections.

As implemented on the IBM 6611, APPN uses data link switching and IP connections to transfer SNA data from a node on one LAN, across a WAN, to a node on another LAN. Data link switching obtains SNA data from a node attached to either a token ring or Ethernet LAN. Depending upon the level of service required by the node requesting the session, the data is either routed through the APPN network node to the Transmission Control Protocol (TCP) or is passed directly to TCP. TCP ensures the reliable (connection-oriented) transfer of data between nodes across a WAN. TCP passes the data to the IP protocol, which transports the data across the WAN.

To configure APPN using the Configuration Program, select the **System Configuration** button on the main menu of the program. APPN is one of the System Configuration options. Within the panels, you can configure the IBM 6611 network node and tune the node's performance based on your needs. Table 3-2 summarizes the options you have when configuring the IBM 6611 network node.

Table 3-2. APPN Configuration Options

IF you want...	THEN...
Minimum Configuration: - Allow the network node to accept any request it receives from another node to establish a connection. - Restrict the network node from initiating connections with other APPN nodes. Note: If you choose the minimum configuration, adjacent nodes must define connections to the IBM 6611 network node to ensure connectivity.	- Configure the following parameters - Network ID - Control point name. - Accept the default (Yes) for the parameter: Accept connection requests from any node. - Select the data link switching connection type from the list and specify a MAC address for this network node. - Accept all other defaults. - Enable the APPN protocol.
To Initiate Connections: - Allow the network node to accept any request it receives from another node to establish a connection. - Enable the network node to initiate connections with other nodes that you specify, including LEN end nodes.	- Configure the following parameters - Network ID - Control point name. - Accept the default (Yes) for the parameter: Accept connection requests from any node. - Select the data link switching connection type from the list and specify a MAC address for this network node. Define which token-ring attached adjacent nodes this network node may initiate a connection with (including LEN end nodes). - Select the IP connection type from the list to specify the IP-attached adjacent nodes with which this network node may initiate a connection. - Enable the APPN protocol.
To Completely Control Connections: - Allow the network node to accept connection requests only from nodes that you specify. - Enable the network node to initiate connections with the nodes that you specify, including LEN end nodes. Note: This option provides a higher level of security because you explicitly define the APPN nodes with which the IBM 6611 can communicate. In addition, this option enables you to have a secure link with each adjacent node by configuring the session level security feature for each link.	- Configure the following parameters - Network ID - Control point name. - Answer No for the parameter: Accept connection requests from any node. - Select the data link switching (data link switching) connection type from the list and specify a MAC address for this network node. Define which token-ring-attached adjacent nodes may communicate with the IBM 6611 network node (required). - Select the IP connection type from the list and specify which IP-attached adjacent nodes may communicate with the IBM 6611 network node (required). - Enable the APPN protocol.

The remainder of this section describes the parameters used to define an IBM 6611 network node and its connections to adjacent nodes.

Network Node Configuration

Enable APPN: This parameter enables or disables this APPN network node. If the node is operating and you disable it, the IBM 6611 stops the APPN protocol.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Network ID: This parameter specifies the name of the APPN network to which this network node belongs. The network ID must be the same for all network nodes in the APPN network. Attached APPN end nodes and LEN end nodes can have different network IDs.

Required: Yes

Dependencies: None

Valid Values: A string of 1 to 8 characters:

First character: A to Z, @, or \$

Second to eighth characters: A to Z, 0 to 9, @, or \$

Note: IBM recommends that the special characters @ and \$ not be used in the network ID unless they are part of an existing network ID that will be used by this node.

Default Value: None

Control Point Name: This parameter specifies the name of the control point (CP) for this APPN network node. The control point is responsible for managing the APPN network node and its resources. The CP name is the logical name of the APPN network node in the network. The CP name must be unique within the APPN network identified by "Network ID."

Required: Yes

Dependencies: None

Valid Values: A string of 1 to 8 characters:

First character: A to Z, @, or \$

Second to eighth characters: A to Z, 0 to 9, @, or \$

Note: IBM recommends that the special characters @ and \$ not be used in the CP name unless this node will be acquiring an existing CP name that contains these characters.

Default Value: None

XID ID Number (Subarea Connection): This parameter specifies a unique ID number (identifier) for this node. The XID ID number is combined with an XID block number (which identifies a specific IBM product) to form an *XID node identification*. Node identifications are exchanged between adjacent nodes when the nodes are establishing a connection. This exchange is referred to as an *exchange station ID (XID)* exchange.

The IBM 6611 network node automatically appends an XID block number to this parameter during the XID exchange to create an XID node identification.

Required: No

Dependencies: Node identifications are normally exchanged between T2.1 nodes during a CP-CP session. If this network node is communicating with the IBM Virtual Telecommunications Access Method (VTAM*) product through a T2.1 LEN node and the LEN node has a CP name defined for it, this parameter is not required. If the adjacent LEN node is not a T2.1 node or does not have an explicitly defined CP name, this parameter is required to establish a connection. VTAM versions prior to Version 3 Release 2 do not allow CP names to be defined for LEN nodes.

The ID number you assign to this node must be unique within the APPN network identified by "Network ID" on page 3-34. Contact your network administrator to verify that the ID number is unique.

Valid Values: A string of 5 hexadecimal digits (0 to 9, A, B, C, D, E, F)

Default Value: 00000

Accept Connection Requests from Any Node: This parameter controls how the IBM 6611 network node responds to a request from another node to establish a connection. When **Yes** is selected, the network node accepts any request it receives from another node to establish a connection. When **No** is selected, the network node accepts connection requests **only** from nodes that you explicitly define. This option provides an added level of security for the IBM 6611 network node.

Required: No

Dependencies: When you choose **No**, you need to explicitly define each node with which this network node may communicate.

- Use the parameters under "Data Link Switching Connection" on page 3-36 to define token-ring-attached nodes that may communicate with this network node using data link switching.
- Use the parameters under "IP Connection" on page 3-41 to define nodes that communicate with this network node across a WAN using an IP connection.

When you choose the default (**Yes**), you may still want this network node to be able to initiate connections with specific nodes. These nodes are also defined using the adjacent node definition parameters for data link switching and IP.

Note: You can define connections with up to 255 adjacent nodes (link stations).

Valid Values: Yes, No (ONLY from explicitly defined nodes)

Default Value: Yes

Data Link Switching Connection

Use the parameters in this section to:

- Define the address of this IBM 6611 network node on the virtual ring used for data link switching. (Refer to the *IBM 6611 Network Processor Introduction and Planning Guide* for a description of how data link switching works.)
- Define adjacent nodes that use data link switching to communicate with this IBM 6611 network node. These adjacent nodes are connected to the IBM 6611 using a token-ring attachment.

You need to define adjacent nodes when:

- You select **No** for “Accept Connection Requests from Any Node” on page 3-35. In this case, you define the nodes with which the IBM 6611 network node may communicate.
- You select the default (**Yes**) for “Accept Connection Requests from Any Node” on page 3-35, but want the IBM 6611 network node to be able to initiate connections with other specific nodes.

Address of This Node for Data Link Switching

The following parameters are specified once and define this network node as part of a virtual ring for data link switching.

MAC Address: This parameter specifies an address in the form of a token-ring medium access control (MAC) address for this APPN network node. The MAC address assigned to this node, combined with the node's SAP address, uniquely identifies the node within a virtual ring defined for data link switching.

Required: Yes

Dependencies: The MAC address and SAP address of this node form an address pair that must be unique within the virtual ring.

Valid Values: A string of 12 hexadecimal digits (0 to 9, A, B, C, D, E, F)

Default Value: None

SAP Address: This parameter specifies a service access point (SAP) address for this APPN network node. The default SAP address (X'04') identifies this node as an APPN node in a data link switching virtual ring.

Required: No

Dependencies: The MAC address and SAP address of this node form an address pair that must be unique within the virtual ring.

Valid Values: X'04' to X'EC', in increments of 4

Default Value: X'04'

Adjacent Node Definitions (Data Link Switching)

The following parameters are configured for each adjacent node you define.

Link Station Name: This parameter specifies the name of the link station that controls the link (transmission group) between this APPN network node and an adjacent node. You can define only one link between the IBM 6611 network node and a specific adjacent node, but each link can carry multiple sessions. The link station name must be unique within this APPN node.

Required: Yes

Dependencies: None.

Valid Values: A string of 1 to 8 characters:

First character: A to Z, @, or \$

Second to eighth characters: A to Z, 0 to 9, @, or \$

Default Value: None

MAC Address: This parameter specifies the MAC address of the adjacent node. The MAC address, combined with the adjacent node's SAP address, uniquely identifies the adjacent node within a virtual ring defined for data link switching.

Required: Yes

Dependencies: The MAC address and SAP address of the adjacent node form an address pair that must be unique within the virtual ring.

Valid Values: A string of 12 hex digits (0 to 9, A, B, C, D, E, F)

Default Value: None

SAP Address: This parameter specifies the SAP address of the adjacent node. The default SAP address (X'04') identifies the adjacent node as an APPN node on a data link switching virtual ring.

Required: No

Dependencies: The MAC address and SAP address of the adjacent node form an address pair that must be unique within the virtual ring.

Valid Values: X'04' to X'EC', in increments of 4

Default Value: X'04'

Activate Link Automatically: When this parameter is enabled, the IBM 6611 network node automatically activates the link to the adjacent node.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Enable Session Level Security: This parameter enables or disables the session level security feature for connections between the IBM 6611 network node and this adjacent node. When the feature is enabled, the IBM 6611 network node will establish a connection with another control point on this link only if the control point has a hexadecimal key that matches the key specified in the parameter “Key” on page 3-38.

The IBM 6611 network node and the adjacent node compare data encrypted using their respective keys to determine if the keys match. This process allows the IBM 6611 network node to verify its partner before proceeding with the connection.

Required: No

Dependencies: When this feature is enabled, you need to define “Key.”

Valid Values: Enable, Disable

Default Value: Disable

Key: This parameter specifies a hexadecimal key that the IBM 6611 network node uses to verify its connection partner. The connection partner must specify an identical key. The IBM 6611 network node and the adjacent node compare data encrypted using their respective keys before establishing a connection. If the data does not match, the IBM 6611 network node does not establish the connection.

It is recommended that the chosen key uniquely identify the link between the IBM 6611 network node and the adjacent node associated with this link station.

Required: See “Dependencies.”

Dependencies: This parameter is required when you enable “Enable Session Level Security.”

Valid Values: A string of up to 16 hexadecimal digits (0 to 9, A, B, C, D, E, F). If fewer than 16 digits are specified, the value is padded on the right with zeros.

Default Value: None

Adjacent Node Type: This parameter identifies whether the adjacent node is an APPN node or a LEN node.

Required: No

Dependencies: When you select **LEN node**, “Fully Qualified Control Point Name” on page 3-39 is a required parameter. If the IBM 6611 network node is communicating with VTAM through the LEN node, and the LEN node does not have a control point or CP name defined for it, “XID Block Number” on page 3-39 and “XID ID Number” on page 3-40 also are required parameters.

Valid Values: APPN node, LEN node

Default Value: APPN node

Fully Qualified Control Point Name: This parameter specifies the adjacent node's fully qualified CP name, which consists of the node's network ID and CP name. The network ID is the name of the network that contains this adjacent node. The CP name is the logical name of this adjacent node and must be unique within the network specified by the network ID.

Required: See "Dependencies."

Dependencies: This parameter is required when:

- You specify **No** for "Accept Connection Requests from Any Node" on page 3-35.
- You specify **LEN node** for "Adjacent Node Type" on page 3-38.

Otherwise, the adjacent node's CP name is learned automatically during the XID exchange between the IBM 6611 network node and the adjacent node. If you specify a CP name when the name is not required, the CP name you specify must match the adjacent node's actual CP name for a connection to be made.

Valid Values: A string of up to 17 characters in the form **netID.CPname**, where:

- **netID** is a network ID from 1 to 8 characters
- **CPname** is a control point name from 1 to 8 characters.

Each name must conform to the following rules:

First character: A to Z, @, or \$

Second to eighth characters: A to Z, 0 to 9, @, or \$

Default Value: None

XID Block Number: This parameter specifies the XID block number associated with the adjacent LEN end node. The XID block number identifies the specific IBM product in the adjacent node that will communicate with this APPN network node. The XID block number is combined with the "XID ID Number" on page 3-40 to form a unique XID node identification for the adjacent node. The nodes use the information provided in the node identifications to determine which link station is the primary link station for the connection.

This parameter is available only when "Adjacent Node Type" on page 3-38 is set to **LEN node**.

Required: No

Dependencies: Node identifications are normally exchanged between T2.1 nodes during a CP-CP session. If this network node is communicating with the VTAM product through a T2.1 LEN node and the LEN node has a CP name defined for it, this parameter is not required. If the adjacent LEN node is not a T2.1 node or does not have an explicitly defined CP name, this parameter is required to establish a connection. VTAM versions prior to Version 3 Release 2 do not allow CP names to be defined for LEN nodes.

Valid Values: A string of 3 hexadecimal digits, with the following values:

- X'01D', if the adjacent LEN node provides a direct connection to VTAM
- X'01E', if the adjacent LEN node provides a connection to VTAM through the IBM Network Control Program (NCP).

Default Value: 000

XID ID Number: This parameter specifies the XID ID number associated with the adjacent LEN end node. The XID ID number serves as a unique identification number for the adjacent node. The XID ID number is combined with the "XID Block Number" to form a unique XID node identification for the adjacent node. Node identifications are exchanged between the IBM 6611 network node and the adjacent node when the nodes are establishing a connection.

This parameter is available only when "Adjacent Node Type" on page 3-38 is set to **LEN node**.

Required: No

Dependencies: Node identifications are normally exchanged between T2.1 nodes during a CP-CP session. If this network node is communicating with the VTAM product through a T2.1 LEN node and the LEN node has a CP name defined for it, this parameter is not required. If the adjacent LEN node is not a T2.1 node or does not have an explicitly defined CP name, this parameter is required to establish a connection. VTAM versions prior to Version 3 Release 2 do not allow CP names to be defined for LEN nodes.

Valid Values: A string of 5 hexadecimal digits (0 to 9, A, B, C, D, E, F)

Default Value: 00000

Fully Qualified LU Name: This parameter specifies the name of an LU in an adjacent LEN node that can be reached through the IBM 6611 network node. When you specify LU names associated with an adjacent LEN node, these names are registered in the IBM 6611 network node's directory database. If you do not register an LU name associated with an adjacent LEN node, the IBM 6611 network node cannot locate that LU (unless the LU name is the same as the CP name of the LEN node).

You need to specify a fully qualified LU name, which consists of a network ID and the LU name. The network ID is the name of the network that contains the adjacent LEN node. The LU name is the name of a logical unit accessible through the adjacent LEN node.

Required: No

Dependencies: This parameter is available only when "Adjacent Node Type" on page 3-38 is set to **LEN node**.

Valid Values: A string of up to 17 characters in the form **netID.LUname**, where:

- **netID** is a network ID from 1 to 8 characters
- **LUname** is an LU name from 1 to 8 characters.

Each name must conform to the following rules:

First character: A to Z, @, or \$

Second to eighth characters: A to Z, 0 to 9, @, or \$

To reduce the number of fully qualified LU names you need to specify, you can use a wildcard character (*) to represent all or a portion of the LU name (**LUname**). A wildcard character cannot be used as part of the network ID (**netID**). The rules for using wildcard characters are:

- A wildcard character can be used to represent the entire LU name (**LUname**). This is a *full wildcard* character. NETA.*, for example, represents all of the LU names associated with the network ID “NETA.” Only one entry containing a full wildcard character may be used within the network specified in the network ID portion of the fully qualified name.
- A wildcard character can be used to represent the second to eighth characters of the LU name. The wildcard character is always the last character in the name. For example, RTP* represents all LU names that begin with the characters RTP.
- An LU name defined with a wildcard character must be unique within the directory of this IBM 6611 network node.

Note: Because a wildcard character can represent numerous resources within your APPN network, you should plan the use of these characters carefully. For example, when performing a broadcast search on behalf of an LU, the IBM 6611 network node accepts the first positive response it receives that the requested LU has been found. This response is used to activate a session. The network node discards any subsequent positive responses that it may receive. If wildcard entries in your network generate multiple responses to the IBM 6611’s broadcast search, the network node could accept an incorrect “resource found” response and discard a valid response.

Default Value: None

IP Connection

Use the parameters in this section to define adjacent nodes that use IP to communicate with this IBM 6611 network node.

You need to define adjacent nodes when:

- You select **No** for “Accept Connection Requests from Any Node” on page 3-35. In this case, you define the nodes with which the IBM 6611 network node may communicate.
- You select the default (**Yes**) for “Accept Connection Requests from Any Node” on page 3-35, but want the IBM 6611 network node to be able to initiate connections with other specific nodes.

Adjacent Node Definitions

The following parameters are configured for each adjacent node you define.

Link Station Name: This parameter specifies the name of the link station that controls the link (transmission group) between this APPN network node and an adjacent node. You can define only one link between the IBM 6611 network node and a specific adjacent node, but each link can carry multiple sessions. The link station name must be unique within this APPN node.

Required: Yes

Dependencies: None

Valid Values: A string of 1 to 8 characters:

First character: A to Z, @, or \$

Second to eighth characters: A to Z, 0 to 9, @, or \$

Default Value: None

IP Address: This parameter specifies the IP address of the adjacent node.

Required: Yes

Dependencies: This IP address must be unique.

Valid Values: The valid ranges for IP address classes are:

Class A	1.0.0.1 through 127.255.255.254
Class B	128.1.0.1 through 191.255.255.254
Class C	192.0.1.1 through 223.255.255.254

Default Value: None

Activate Link Automatically: When this parameter is enabled, the IBM 6611 network node automatically activates the link to the adjacent node.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Enable Session Level Security: This parameter enables or disables the session level security feature for connections between the IBM 6611 network node and this adjacent node. When the feature is enabled, the IBM 6611 network node will establish a connection with another control point on this link only if the control point has a hexadecimal key that matches the key specified in the parameter "Key" on page 3-38.

The IBM 6611 network node and the adjacent node compare data encrypted using their respective keys to determine if the keys match. This process allows the IBM 6611 network node to verify its partner before proceeding with the connection.

Required: No

Dependencies: When this feature is enabled, you need to define "Key" on page 3-38.

Valid Values: Enable, Disable

Default Value: Disable

Key: This parameter specifies a hexadecimal key that the IBM 6611 network node uses to verify its connection partner. The connection partner must specify an identical key. The IBM 6611 network node and the adjacent node compare data encrypted using their respective keys before establishing a connection. If the data does not match, the IBM 6611 network node does not establish the connection.

It is recommended that the chosen key uniquely identify the link between the IBM 6611 network node and the adjacent node associated with this link station.

Required: See "Dependencies."

Dependencies: This parameter is required when you enable “Enable Session Level Security” on page 3-38.

Valid Values: A string of up to 16 hexadecimal digits (0 to 9, A, B, C, D, E, F). If fewer than 16 digits are specified, the value is padded on the right with zeros.

Default Value: None

Fully Qualified Control Point Name: This parameter specifies the adjacent node’s fully qualified CP name, which consists of the node’s network ID and CP name. The network ID is the name of the network that contains this adjacent node. The CP name is the logical name of this adjacent node and must be unique within the network specified by the network ID.

Required: No

Dependencies: This parameter is required when you specify **No** for “Accept Connection Requests from Any Node” on page 3-35. Otherwise, the adjacent node’s CP name is learned automatically during the XID exchange between the IBM 6611 network node and the adjacent node. If you specify a CP name when the name is not required, the CP name you specify must match the adjacent node’s actual CP name for a connection to be made.

Valid Values: A string of up to 17 characters in the form **netID.CPname**, where:

- **netID** is a network ID from 1 to 8 characters
- **CPname** is a control point name from 1 to 8 characters.

Each name must conform to the following rules:

First character: A to Z, @, or \$

Second to eighth characters: A to Z, 0 to 9, @, or \$

Default Value: None

Tuning an IBM 6611 Network Node

You can tune the performance of the IBM 6611 network node by determining the values of the following parameters: “Maximum Shared Memory” on page 3-45 and “Maximum Cached Directory Entries” on page 3-46. The Configuration Program automatically generates a table of values for these parameters and enables you to select which set of values to use (automatic tuning). Each set of values corresponds to a choice for tuning the network node.

Five tuning options are available. The first tuning option yields the **best performance**, which requires more storage. The last tuning option provides for **minimum storage usage**. The default tuning option, **balanced adjustment**, is a balance between best performance and minimum storage usage. The other tuning options represent more gradual steps along the range.

The table of values generated by the Configuration Program is based on your responses to (or default settings of) the following tuning default parameters:

- “Maximum Number of Network Nodes in Your APPN Network” on page 3-44
- “Maximum Number of End Nodes and LEN Nodes Serviced by This Node” on page 3-44
- “Average Number of LUs Associated with End Nodes and LEN Nodes Serviced by This Node” on page 3-44.

Note: When you change the value of any one of the tuning default parameters, a new set of values is calculated for the tuning table when you either:

- Press the Enter key
- Press the Tab key
- Click the mouse
- Select the OK button.

If you prefer, you can manually tune the performance of the IBM 6611 network node by select the Manual tuning option of the panel and entering your own values for “Maximum Shared Memory” on page 3-45 and “Maximum Cached Directory Entries” on page 3-46.

Maximum Number of Network Nodes in Your APPN Network: This parameter is an *estimate* of the maximum number of network nodes that you expect to support in the APPN network identified by the parameter “Network ID” on page 3-34.

This parameter is used to calculate a range of values for the “Maximum Shared Memory” and “Maximum Cached Directory Entries” parameters. An estimate is used to enable you to compensate for expected growth in your network.

Required: No

Dependencies: None

Valid Values: 50 to 65535

Note: If the number you specify is too large for your network, the Maximum shared memory allocation may be excessive for your configuration. The Configuration program tuning panel shows the amount of shared memory that is allocated.

Default Value: 100

Maximum Number of End Nodes and LEN Nodes Serviced by This Node: This parameter is an *estimate* of the maximum number of APPN end nodes and LEN end nodes that you expect to attach to this IBM 6611 network node.

This parameter is used to calculate a range of values for the “Maximum Shared Memory” and “Maximum Cached Directory Entries” parameters. An estimate is used to enable you to compensate for expected growth in your network.

Required: No

Dependencies: None

Valid Values: 10 to 65535

Default Value: 500

Average Number of LUs Associated with End Nodes and LEN Nodes Serviced by This Node: This parameter specifies the average number of LUs associated with adjacent nodes connected to this IBM 6611 network node.

This parameter is used to calculate a range of values for the “Maximum Shared Memory” and “Maximum Cached Directory Entries” parameters. The simplest way to calculate this value is to divide the total number of adjacent node LUs by the number of adjacent nodes connected to the IBM 6611 network node. When

determining the number of LUs associated with an adjacent LEN end node, use the number of LUs that are registered in the IBM 6611 network node's local directory.

Note: You can estimate the number of LUs associated with an adjacent node. More exact estimates yield more accurate tuning information.

Required: No

Dependencies: None

Valid Values: 1 to 65535

Default Value: 2

Maximum Shared Memory: This parameter specifies the amount of shared memory within the IBM 6611 that is allocated to the APPN network node. APPN uses its shared memory allocation to perform network operations and to maintain required tables and directories.

Because this parameter affects storage allocation within the IBM 6611, you should use care when changing this value. Use the values provided within the Configuration program tuning table as a guide when increasing or reducing Maximum shared memory or select a tuning option within the table that is appropriate for your network's needs.

Note: The actual amount of shared memory available to the APPN network node will be limited by the available disk space on the IBM 6611 and the number of other protocols running on the device.

Required: No

Dependencies: The value of this parameter is automatically calculated by the Configuration program tuning table. If you prefer, however, you can manually tune the performance of the IBM 6611 network node by selecting the Manual tuning option on the panel and entering an explicit value for this parameter.

Valid Values: 2 to 40 megabytes

Default Value: The default value for this parameter is the same as the current value of the parameter displayed within the automatic tuning table.

Maximum Cached Directory Entries: This parameter specifies the number of entries stored or *cached* in the IBM 6611 network node's local directory. After successfully locating a resource in the network, the network node caches information about the resource in its local directory for future reference. With a large number of cached directory entries, the network node needs to issue fewer broadcast searches, reducing network overhead and leading to faster session establishment. A large cache, however, requires additional storage and may include entries that are no longer valid.

Required: No

Dependencies: The value of this parameter is automatically calculated by the Configuration program tuning table. If you prefer, however, you can manually tune the performance of the IBM 6611 network node by selecting the Manual tuning option on the panel and entering an explicit value for this parameter.

Valid Values: 10 to 65535

Default Value: The default value for this parameter is the same as the current value of the parameter displayed within the automatic tuning table.

NetBIOS

Use the worksheet on page A-3.

Network Basic Input/Output System (NetBIOS) is a local area network (LAN) protocol used to communicate between two stations on a LAN. The user must assign each station a NetBIOS name. NetBIOS establishes a connection-oriented session between two NetBIOS names.

You must configure the following functions when you want NetBIOS support on an IBM 6611:

- A LAN adapter (Token-Ring Network 16/4 Adapter or Ethernet Adapter)
- IP on at least one port
- Enable the data link switching NetBIOS frame forwarding function
- For NetBIOS over a Token-Ring Network 16/4 Adapter, the token-ring port must be configured for bridging.
- Data link switching must be configured.

List of NetBIOS Default Destinations

The following parameters define which IBM 6611 provides routing services for a NetBIOS node. Each NetBIOS node may have one or more IBM 6611s defined as the default router, and each IBM 6611 may provide routing services for multiple NetBIOS nodes.

IP Address of Destination Router: This parameter defines an IBM 6611 used in a search for the the destination NetBIOS node.

Required: No

Dependencies: This parameter is required to define NetBIOS default destinations.

Valid Values: Any router address configured in "IP Address of Remote IBM 6611" on page 3-26.

Default Value: None

Destination Name: This parameter contains the destination name that identifies the NetBIOS node serviced by the IBM 6611 specified in "IP Address of Destination Router." A wildcard character (*) can be used to match any characters at the end of a name.

Required: No

Dependencies: This parameter is required to define NetBIOS default destinations.

Valid Values: Any valid NetBIOS name

Default Value: None

NetBIOS Name Filters

NetBIOS allows the user to define a set of filters which are applied to NetBIOS frames that are transported using data link switching. Each filter is composed of a source name and destination name. The filter compares the source name and destination name of each NetBIOS explorer frame with the configured list. *Explorer frames* are frames that are used to resolve a logical name to a MAC address. The purpose of filtering is to allow or disallow connection establishment between NetBIOS stations. Filters are not applied to data frames sent after a connection is established. Unlike bridge filtering, data link switching filtering does not cause a performance impact.

NetBIOS Source Name Filters

NetBIOS source name filters are applied to explorer frames traveling from a LAN connection to a WAN connection.

Status of All Defined NetBIOS Source Name Filters: This parameter enables or disables all defined NetBIOS source name filters. When NetBIOS source name filters are not configured, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Source Name Filter Type: This parameter specifies the type of all NetBIOS source name filters for this IBM 6611. You can select either deny or permit.

When the value of this parameter is set to **Deny**, every frame whose source name and destination name match a configured source name and destination name is not allowed to use data link switching. When the value of this parameter is set to **Permit**, only those frames whose source name and destination name match a configured source name and destination name are allowed to use data link switching.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Permit

List of NetBIOS Source Name Filters

Source Name: This parameter contains the source name used in NetBIOS source name filters.

Required: No

Dependencies: This parameter is required to define NetBIOS source name filters.

Valid Values: Any valid NetBIOS name

Default Value: None

Destination Name: This parameter contains the destination name used in NetBIOS source name filters.

Required: No

Dependencies: This parameter is required to define a NetBIOS source name filter.

Valid Values: Any valid NetBIOS name

Default Value: None

NetBIOS Destination Name Filters

NetBIOS destination name filters are applied to explorer frames traveling from a WAN connection to a LAN connection.

Status of All Defined NetBIOS Destination Name Filters: This parameter enables or disables all configured NetBIOS destination name filters. When NetBIOS destination name filters are not configured, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Destination Name Filter Type: This parameter indicates the type of all NetBIOS destination name filters for this IBM 6611. You can select either deny or permit.

When this parameter is set to **Deny**, every frame whose source name and destination name match a configured source name and destination name is not allowed to use data link switching. When this parameter is set to **Permit**, only those frames whose source name and destination name match a configured source name and destination name are allowed to use data link switching.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

List of NetBIOS Destination Name Filters

Source Name: This parameter contains the source name used in NetBIOS destination name filters.

Required: No

Dependencies: This parameter is required to define NetBIOS destination name filters.

Valid Values: Any valid NetBIOS name

Default Value: None

Destination Name: This parameter contains the destination name used in NetBIOS destination name filters. A wildcard character (*), which matches any number of characters at the end of a name, is allowed.

Required: No

Dependencies: This parameter is required to define a NetBIOS destination name filter.

Valid Values: Any valid NetBIOS name

Default Value: None

IP Routing Protocols

The IBM 6611 implements the following IP routing protocols: Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Hello, Border Gateway Protocol (BGP), and Exterior Gateway Protocol (EGP). In addition, static routes also may be configured manually.

Because there is the possibility that more than one of the protocols may provide routes to the same destination, you can indicate ahead of time which protocol (including static) is preferable. It is called the *route preference* and can be any value from 0 to 255. A preference of 0 is the most preferred. The preference of each protocol can be configured. The default values are listed in the sections below. It is not possible to have more than one route to a destination from the same protocol. Therefore, it is not possible to prefer one static route over another, for instance.

OSPF

Use the worksheet on page A-5.

Enable OSPF: This parameter enables or disables OSPF.

Required: No

Dependencies: You must configure IP addresses before you can configure OSPF.

Valid Values: Enable, Disable

Default Value: Disable

Router ID: This parameter is used by OSPF to identify this router uniquely.

Required: Yes

Dependencies: None

Valid Values: An IP address configured for this IBM 6611.

Default Value: None

List of OSPF Areas

Area ID: An *area* is a group of connected networks, hosts, and specific router interfaces. An area can be described as the generalization of a subnetted network. An area can be a transit area or non-transit area (stub area). A *transit area* is an area that is attached to more than one other area and therefore can be used for transit traffic between areas. A *non-transit area*, or stub area, can be attached to only one other area, which is the OSPF backbone. A non-transit area can be configured to import a default route to the non-transit area's border router. This allows all routers within an area to use the area border router as the default path to any network that cannot be reached within the area.

Required: No

Dependencies: If an area ID other than 0.0.0.0 is selected, then the non-transit and cost entry parameters are displayed.

Valid Values: 0.0.0.0 to 255.255.255.255

Default Value: 0.0.0.0

Area Type: This parameter defines whether an area is transit or non-transit. A *transit area* is an area that is attached to more than one other area and therefore can be used for transit traffic between areas. A *non-transit* (stub) area is attached to only one other area, which is the OSPF backbone. A non-transit area can be configured to import a default route to its area border router. This is done by configuring a non-transit cost for this area. This allows all routers within this area to use that area border router as the default path to any network that cannot be reached within this area. Autonomous system external routes are not flooded within a non-transit area.

Required: No

Dependencies: None

Valid Values: Transit, Stub

Default Value: Transit

Stub Cost: An area may be a transit area or stub area (non-transit area). A transit area is an area that is attached to more than 1 other area and therefore can be used for transit traffic (between areas).

A stub area is attached to only 1 other area, which is the OSPF backbone.

A stub area may be configured to import a default route to its area border router. This is done by configuring the stub cost for this area.

Required: No

Dependencies: None

Valid Values: 1 to 65535

Default Value: None

Authentication Type: The authentication type for an area defines whether the OSPF protocol packets are authenticated. When simple password authentication is used, a password must be defined.

Required: No

Dependencies: When this parameter is set to **Simple**, "Authorization Key" on page 3-53 is required.

Valid Values: None, Simple

Default Value: None

List of OSPF Interfaces

Interface IP Address: This is a read-only list of the configured IP addresses for the IBM 6611. Select the IP addresses to modify the configuration. New addresses cannot be added using this parameter.

Required: Yes

Dependencies: This parameter is configured for each interface.

Valid Values: All configured IP addresses for the IBM 6611.

Default Value: All configured IP addresses on the IBM 6611 in a list window of the Configuration Program.

Interface Type: This parameter defines whether this interface is a broadcast or non-broadcast media.

Required: No

Dependencies: None

Valid Values: Broadcast, Non-broadcast

Default Value: Broadcast

Authorization Key: This parameter defines the authorization key for this interface.

Required: No

Dependencies: Authentication type must not be set to **None**. This parameter is configured for each interface.

Valid Values: Any 8 characters

Default Value: None

Router Priority: This parameter is used in broadcast and non-broadcast multi-access networks to select the designated router. For point-to-point links, this value should be 0. A 0 value means that this router must not be selected as the designated router for its network.

Required: No

Dependencies: This parameter is configured for each interface.

Valid Values: 0 to 255

Default Value: 1

Cost: This parameter defines the cost that OSPF associates with the interface. The cost is used to determine the shortest path to the network. Lower costs are preferred.

Required: No

Dependencies: None

Valid Values: 1 to 65535

Default Value: 1

Poll Interval: This parameter sets the interval that OSPF Hello packets are sent to a neighbor that is inactive. This means that Hello packets have not been sent by the neighbor for "Router Dead Interval" on page 3-54.

Required: No

Dependencies: This data entry field is for non-broadcast, multi-access interface only.

Valid Values: 1 to 255

Default Value: 120

Retransmit Interval: This parameter identifies the frequency of retransmitting link-state update packets, link-state request packets, and database description packets.

Required: No

Dependencies: None

Valid Values: 1 to 3600 seconds

Default Value: 5 seconds

Interface Transit Delay: This parameter defines the minimum delay for an interface as 1 second. Each link-state advertisement has a finite lifetime, which is equal to the constant MaxAge (1 hour). As each link-state advertisement is sent out on particular interfaces, it is aged by this configured delay.

Required: No

Dependencies: None

Valid Values: 1 to 3600 seconds

Default Value: 1 second

Router Dead Interval: When an OSPF Hello is not received from a neighboring router by the time defined in this parameter, the neighbor is declared to be inoperative. The value of this parameter must be the same as the neighbor router's router dead interval parameter.

Required: No

Dependencies: None

Valid Values: 1 to 65535 seconds

Default Value: 40 seconds

Hello Interval: This parameter defines the frequency of sending OSPF Hello packets. This value must be the same as the neighbor router's Hello interval.

Required: No

Dependencies: None

Valid Values: 1 to 255 seconds

Default Value: 10 seconds

Interface Type: This parameter defines the minimum delay for an interface as 1 second. Each link-state advertisement has a finite lifetime, which is equal to the constant MaxAge (1 hour). As each link-state advertisement is sent out on particular interfaces, it is aged by this configured delay.

Required: No

Dependencies: None

Valid Values: Broadcast, Non-Broadcast

Default Value: Broadcast

List of OSPF Neighbors

IP Address of Neighbor Router: This parameter defines the IP address of an OSPF Neighbor Router on a non-broadcast, multi-access network.

Required: Yes

Dependencies: This parameter is configured for each OSPF neighbor.

Valid Values: A valid IP address

Default Value: None

Eligible to Become a Designated Router: This parameter indicates that the router specified in “IP Address of Neighbor Router” is eligible to become the designated router for this network.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

OSPF List of Network Ranges

Network Number: Configuring OSPF areas allows for compacted network information. This is important for large OSPF autonomous systems. The compacted network information is located at the area border router. The network ranges are advertised by the area border router into other areas. For example, if an area includes the networks 128.8.9.0, 128.8.10.0, 128.8.20.0, and 128.8.21.0, the address range 128.8.0.0 with network mask 255.255.0.0 causes only 128.8.0.0 to be advertised as a summary link-state advertisement to the other area.

Required: Yes

Dependencies: This parameter and “Network Mask” are configured for each network number that is defined.

Valid Values: A valid IP network address

Default Value: None

Network Mask: This parameter defines the mask for each network number that is configured.

Required: Yes

Dependencies: None

Valid Values: A valid IP network mask

Default Value: 255.255.255.0

OSPF List of Virtual Links

The following parameters are configured for each virtual link.

Virtual Link ID: This parameter uniquely identifies this virtual link.

Required: Yes

Dependencies: This parameter is required to configure a virtual link.

Valid Values: A string of 1 to 16 alphanumeric characters.

Default Value: None

Virtual Neighbor ID: The parameter identifies the router ID of the virtual neighbor.

Required: Yes

Dependencies: This parameter is required to configure a virtual link.

Valid Values: 0.0.0.0 to 255.255.255.255

Default Value: None

Transit Area ID: This parameter must be one of this area border router's adjacent configured transit areas.

Required: Yes

Dependencies: This parameter is required to configure a virtual link.

Valid Values: 0.0.0.1 to 255.255.255.255

Default Value: None

Authorization Key: This parameter defines the authorization key for this interface. This parameter is configured when "Authentication Type" on page 3-52 is set to **Simple**. This parameter assigns an authentication key.

Required: No

Dependencies: Authentication type must not be set to **None**. This parameter is configured for each interface.

Valid Values: Any 8 characters

Default Value: None

Retransmit Interval: This parameter determines the frequency of retransmitting link-state update packets, link-state request packets, and database description packets.

Required: No

Dependencies: None

Valid Values: 1 to 3600 seconds

Default Value: 5 seconds

Interface Transit Delay: This parameter defines the configured delay that ages the link state advertisement that is sent to particular interfaces.

Required: No

Dependencies: None

Valid Values: 1 to 3600 seconds

Default Value: 1 second

Router Dead Interval: When an OSPF Hello is not received from a neighboring router by the time defined in the router dead interval, the neighbor is declared to be inactive. The value of this parameter must be the same as the virtual neighbor router's router dead interval parameter.

Required: No

Dependencies: This parameter is configured for each interface.

Valid Values: 1 to 65535 seconds

Default Value: 60 seconds

Hello Interval: This parameter determines the frequency with which OSPF Hello Packets are sent. This value must be the same as the virtual Neighbor Router Hello Interval.

Required: No

Dependencies: This parameter is configured for each interface.

Valid Values: 1 to 255 seconds

Default Value: 10 seconds

Routing Information Protocol

Use the worksheet on page A-6.

The Routing Information Protocol (RIP) is a routing protocol that uses the User Datagram Protocol (UDP) to exchange routing information between routers. RIP uses a metric called a *hop count* to measure the distance of each RIP route. The *hop count* is an integer from 0 to 16. A hop count of zero indicates that the destination network is directly attached to the IBM 6611. A hop count of 16 means that the destination network cannot be reached from an IBM 6611. Therefore, a RIP internet cannot have valid routes longer than 15 hops.

The operation of RIP involves broadcasting of routing information every 30 seconds on each interface that is configured to send RIP information. Other routers in the network that also are running RIP read the broadcasts containing the RIP information and update their route tables according to the information received. This allows for alternate route recovery if links become unavailable.

By default, RIP is disabled. The optional RIP parameters allow the network administrator to tailor on which IP interfaces RIP information should be sent and from which it should be received. The parameters on route metrics and preference control how the RIP routes are used.

Restrictions: None

Enable Routing Information Protocol (RIP): This parameter enables or disables RIP on defined IP interfaces.

Required: No

Dependencies: IP must be configured. RIP can be configured only on an adapter port running IP.

Valid Values: Enable, Disable

Default Value: Disable

Broadcast: When this parameter is set to **Enable**, it ensures that RIP packets are broadcast on all RIP enabled interfaces. When this parameter is set to **Disable**, the RIP packets are sent to routers defined in the list of source routers.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Zero Reserved Fields: When this parameter is set to **Enable**, it ensures that RIP verifies that unused fields in RIP packets are zero. When this parameter is set to **Disable**, reserve fields cannot be changed.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Route Preference: This parameter defines the preference value for routes learned by RIP. This value is used to determine the route when multiple routes to the same destination exist. The route with the lowest preference value is used.

Required: No

Dependencies: RIP can be configured only on an adapter port running IP.

Valid Values: 0 to 255, 0 being the most preferred route.

Default Value: 100

List of RIP Source Routers

IP Address of Source Router: This parameter determines which routers are sent RIP messages. It defines the routers that receive RIP messages when "Broadcast" on page 3-58 is set to **Disabled**.

Required: Yes

Dependencies: None

Valid Values: A valid IP address

Default Value: None

RIP Interface Settings

IP Address of Local Interface: This parameter displays an IP address of an interface on this IBM 6611 that was selected from a list in the Configuration Program.

Required: Yes

Dependencies: This IP address parameter, "Listen for RIP Updates," and "Send RIP Updates" on page 3-60 defines the way in which RIP updates are processed for each interface.

Valid Values: A valid IP address

Default Value: None

Listen for RIP Updates: This parameter determines whether RIP messages are accepted on this interface.

Required: No

Dependencies: This parameter, "Listen for RIP Updates," and "Send RIP Updates" on page 3-60 define the way in which RIP updates are processed for each interface.

Valid Values: Enable, Disable

Default Value: Enable

Send RIP Updates: This parameter determines whether RIP messages are sent on this interface.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

List of RIP Trusted Routers

IP Address of Trusted Router: This parameter specifies the router whose list of advertised routes is trusted. When any router is listed, the routes advertised by any unlisted router are discarded. When this parameter is not configured, all routers are trusted.

Required: No

Dependencies: This parameter is required to define RIP trusted routers.

Valid Values: A valid IP address

Default Value: None

List of RIP Imports

Name of Import Filter: This parameter defines a name for each RIP import filter.

Required: No

Dependencies: This parameter is required to define RIP import filters.

Valid Values: Any alphanumeric string up to 16 characters in length.

Default Value: None

List of RIP Import Destinations

Destination: This parameter defines the destination IP address for this RIP import filter.

Required: Yes

Dependencies: None

Valid Values: A valid IP address

Default Value: None

Destination Mask: This parameter defines the mask that is applied to the IP address to define a range of IP addresses that are imported.

Required: No

Dependencies: This parameter is required to define RIP import destinations.

Valid Values: A valid IP address mask (0.0.0.0 to 255.255.255.255)

Default Value: 255.255.255.255

Preference: This parameter defines the preference attached to all RIP routes that are imported with the set of addresses specified by the “Destination” and “Destination Mask” parameters. Zero means most preferred.

Required: No

Dependencies: None

Valid Values: 0 to 255

Default Value: 100

Restrict: This parameter defines when the routes defined by the destination IP address (“Destination” on page 3-60) and the mask (“Destination Mask” on page 3-60) are restricted from being added to the local route table.

Required: No

Dependencies: If this parameter is set to **Enable**, all other routes that should not be restricted should be entered with a preference value.

Valid Values: Enable, Disable

Default Value: Disable

Filter Routes from: This parameter defines when the route imports are applied to local IP interfaces or remote routers. When **All sources** is selected, the RIP updates received on any local IP interface are added into the local route table. When **Interface** is selected, you can enter one or more IP addresses of local interfaces from which routes are imported to the local routing table. Likewise, when **Remote router** is selected, you can select one or more IP addresses of remote routers.

Required: No

Dependencies: None

Valid Values: All sources, Remote router, Interface

Default Value: All sources

List of RIP Import Routers

IP Address of Remote Router: This parameter defines an IP address of a remote router that is used to receive RIP updates.

Required: Yes

Dependencies: This parameter must be configured for each RIP import filter that selects **Remote Router** in “Filter Routes from.”

Valid Values: A valid IP address

Default Value: None

List of RIP Import Interfaces

IP Address of Local Interface: This parameter defines the IP address of any local interface that is configured for IP.

Required: Yes

Dependencies: This parameter is required when “Filter Routes from” on page 3-61 is set to **Interface**. You must configure this parameter once for each RIP import filter set to **Interface**.

Valid Values: A valid IP address of a local interface

Default Value: None

Hello Protocol

Use the worksheet on page A-7.

Hello protocol is an IP interior gateway protocol. Hello, like RIP, broadcasts its routing information. Instead of using a hop count routing metric like RIP, Hello uses a network delay routing metric to represent the time that elapses to send a packet from the IBM 6611 to the destination network using the route. The metric assigned to the IBM 6611 by Hello can be a value of 0 to 30 000 milliseconds. 30 000 milliseconds means that the destination is considered unattainable. At each router, the Hello algorithm calculates delays for destinations and selects the router with the shortest delay for the pathway.

Hello is set to **Disable** by default. When Hello is enabled, it is sent and received on all IP interfaces.

Restrictions: Hello can be configured only on a port configured for IP.

Enable Hello Protocol: This parameter enables or disables using the Hello protocol on defined IP ports.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Broadcast: When this parameter is enabled, Hello packets are broadcast on all Hello enabled interfaces. When this parameter is disabled, the Hello packets are sent only to gateways in the list of source routers.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Route Preference: This parameter defines the preference value for routes learned by Hello. This value is used to determine the route to use when multiple routes to the same destination exist. The route with the lowest preference value is used.

Required: No

Dependencies: None

Valid Values: 0 to 255

Default Value: 90

List of Hello Source Routers

IP Address of Source Router: This parameter defines a source router. It defines the routers that receive Hello messages when "Broadcast" is set to **Disabled**.

Required: Yes

Dependencies: This parameter is required to define Hello source routers.

Valid Values: A valid IP address

Default Value: None

Hello Interface Settings

IP Address of Local Interface: This parameter displays the IP address of a port on this router that was selected from a displayed list. This IP address and the values for "Listen for Hello Updates" and "Send Hello Updates" provides the information needed to complete each interface.

Required: Yes

Dependencies: This parameter is required to define Hello interface settings.

Valid Values: A valid IP address

Default Value: IP address that was selected from a list window in the Configuration Program.

Listen for Hello Updates: This parameter defines when Hello messages are accepted on the port.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Send Hello Updates: This parameter defines whether Hello messages are sent on this interface.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

List of Hello Trusted Routers

IP Address of Trusted Router: This parameter specifies the routers whose list of advertised routes are trusted. If any router is listed, the routes advertised by any unlisted router are discarded. When this parameter is omitted, all routers are trusted.

Required: No

Dependencies: This parameter is required to define trusted Hello routers.

Valid Values: A valid IP address

Default Value: None

List of Hello Imports

Name of Import Filter: This parameter defines a name for each Hello import filter.

Required: No

Dependencies: This parameter is required to define Hello imports.

Valid Values: Any alphanumeric string up to 16 characters in length

Default Value: None

List of Hello Import Destinations

Destination: This parameter defines the destination IP address for this Hello import filter.

Required: Yes

Dependencies: None

Valid Values: A valid IP address

Default Value: None

Destination Mask: This parameter defines the mask that is applied to "Destination" to define a range of destinations that are imported.

Required: No

Dependencies: None

Valid Values: A valid IP address mask (0.0.0.0 to 255.255.255.255)

Default Value: 255.255.255.255

Preference: This parameter defines the preference attached to all Hello routes that are imported with the set of addresses specified by parameters. Zero is most preferred.

Required: No

Dependencies: None

Valid Values: 0 to 255

Default Value: 90

Restrict Routes: This parameter defines when the routes defined by the destination IP address and mask ("Destination" and "Destination Mask" parameters) are restricted from being added to the local route table.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Filter Routes from: This parameter defines whether route imports are applied routes learned from all sources, a specific local IP interface, or remote routers. When **All sources** is selected, the Hello updates received on any local IP interface are added to the local route table. When **Interface** is selected, you can enter one or more IP addresses of local interfaces from which routes are imported into the local routing table. When **Remote routers** is selected, you can select one or more IP addresses of remote routers.

Required: No

Dependencies: None

Valid Values: All sources, Remote routers, Interface

Default Value: All sources

Hello Import Routers

IP Address of Remote Router: This parameter is an IP address of a remote router that is used to receive Hello route updates.

Required: No

Dependencies: This parameter must be configured for each remote router. This parameter is required to define the Hello import routers.

Valid Values: A valid IP address

Default Value: None

List of Hello Import Interfaces

IP Address of Local Interface: This parameter identifies the IP address of any local interface that is configured for IP.

Required: No

Dependencies: This parameter must be configured for each interface. This parameter is required when "Filter Routes from" is set to **Interface**.

Valid Values: IP address of local interface

Default Value: None

Border Gateway Protocol (BGP)

Use the worksheet on page A-8.

The BGP is an inter-autonomous system routing protocol for exchanging network reachability information.

A BGP router exchanges information about the networks that it can reach. That information is used to construct a graph of the entire autonomous system, which facilitates detection and elimination of problems, such as routing loops.

BGP uses TCP to establish a connection between two BGP neighbors (in this case, the IBM 6611 and another router using BGP). After the TCP connection has been established, the BGP neighbors exchange their full routing tables. After the initial exchange of routing tables, the BGP neighbors exchange only changes to the routing tables. For each network that can be reached via the BGP neighbor, the routing table indicates the complete autonomous system path to the network.

BGP uses a policy-based algorithm to determine the best path to an autonomous system. The routing policies used by the algorithm are based partly on the information you specify during configuration of the router.

Using the Configuration Program, you will:

1. **Specify the global default parameters.**

You will specify, on the BGP panel, the parameter values to be applied to the IBM 6611. These parameter values establish the global default values for each BGP group that you define.

2. **Specify the BGP group and BGP neighbor parameters.**

On the BGP Group Detail panel, you will define each BGP group. For each BGP group, you will specify the BGP neighbors in the group. At least one BGP neighbor (configured or unconfigured) must be specified per BGP group. The BGP group values establish the default values for the BGP neighbors in the group.

3. **Specify the BGP import filter parameters.**

On the BGP Import Detail panel, you will specify the BGP import filter parameters for each autonomous system from which routes are to be imported.

BGP Global Default Parameters

BGP global default parameters apply to all defined BGP groups.

Enable Border Gateway Protocol (BGP): This parameter enables or disables BGP on the IBM 6611.

Required: Yes (if you use BGP)

Dependencies: BGP can be configured only on interfaces that have been configured for the Internet Protocol (IP).

If BGP is enabled, the “Local Autonomous System Number” on page 3-68 and “Autonomous System Number – ASN” on page 3-69 of a remote autonomous system must be specified.

Within the remote autonomous system, at least one “BGP Group Type” on page 3-69 must be specified. Within each BGP group exists one or more routers, referred to as *BGP configured* or *unconfigured neighbors*, that use BGP to exchange their current routing information with the IBM 6611. Within each BGP group that is specified, at least one configured or unconfigured neighbor must be specified.

Valid Values: Enable, Disable

Default Value: Disable

Generate Default Route: This parameter, when enabled, generates a default route pointer to an IBM 6611. This route can be exported to other routers using the protocol default.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Local Autonomous System Number: This parameter defines the autonomous system number of the IBM 6611.

Required: Yes (if “Enable Border Gateway Protocol (BGP)” on page 3-67 is set to **Enable**)

Dependencies: None

Valid Values: 1 to 65534

Default Value: None

Default Preference (0 – 255): This parameter defines the preference value that BGP assigns to all routes learned by the IBM 6611 (unless a preference is assigned to a particular BGP group, BGP configured neighbor, or BGP import). If you do not specify a value, BGP uses a value of 150.

BGP uses the preference value to determine which route to use when multiple routes to the same destination exist. The route with the lowest preference value will be used.

Required: No

Dependencies: None

Valid Values: 0 to 255 (with the lowest value being the most preferred)

Default Value: None

Default Metric: This parameter specifies the default metric used by BGP when propagating routes learned from other protocols (for example, OSPF).

Required: No

Dependencies: None

Valid Values: 0 to 65535

Default Value: None

BGP Group Parameters

The BGP group parameters are specified once for each BGP group defined and provide defaults for the BGP configured and unconfigured neighbors within the BGP group.

Note: BGP group parameters override BGP global default parameters.

Autonomous System Number – ASN: The neighbors in the BGP group must reside in an autonomous system. This parameter specifies the autonomous system number of the neighbors' autonomous system.

Required: Yes

Dependencies: None

Valid Values: 1 to 65534

Default Value: None

BGP Group Type:

External: This is an external BGP group. BGP neighbors in an external BGP group must be directly reachable through one of the IBM 6611's interfaces. (The network portion of their IP addresses must be the same.)

Test: A special case of external BGP group type. The IBM 6611 discards all routing information advertised to it by a BGP neighbor in a test group and sends all BGP-advertisable routes back to the neighbor in the test group.

BGP neighbors in a test group do not have to be on the same physical network. (The network portion of their IP addresses does not have to be the same.) If the IBM 6611 and the BGP neighbors in the test group are on the same physical network, the next hop is computed with respect to the network; otherwise, the next hop is the IBM 6611's current next hop. Metrics from BGP- and EGP-derived routes are forwarded in the advertisement; otherwise, no metric is included in the advertisement.

Internal: This type of internal group operates where there is no IP-level IGP (for example, over the Military Network [MILNET]). Neighbors in an internal group must be directly reachable through one of the IBM 6611's interfaces, and the next hop is computed with respect to the interface. Advertisements received from internal neighbors in the same group are never advertised.

IGP: Neighbors in this type of internal group examine routes that OSPF is exporting and send an advertisement only if the path attributes could not be represented in the OSPF tag. Only the autonomous system path, autonomous system path origin, and transitive optional attributes are sent with routes. A metric is not sent, and the next

hop is set to the address used by the connection between the IBM 6611 and the IGP group. Neighbors in an IGP group do not have to be directly reachable through one of the IBM 6611's interfaces (for example, another router can be between the IBM 6611 and an IGP group). Received IGP routes are never used or re-advertised by BGP. Instead, the autonomous system path information is attached to the corresponding IGP route and the IGP route is used for re-advertisement.

Required: No

Dependencies: None

Valid Values: External, Test, Internal, IGP

Default Value: External

BGP Group Name: This parameter specifies a user-defined name for a BGP group.

Required: No

Dependencies: None

Valid Values: Any alphanumeric from 1 to 16 digits in length

Default Value: None

Metric Out: This parameter specifies the default metric given by the IBM 6611 to all routes propagated to the BGP group. This parameter is ignored for IGP groups. (See "BGP Group Type" on page 3-69.)

Required: No

Dependencies: None

Valid Values: 0 to 65535

Default Value: None

Next Hop Destination: This parameter specifies the IP address of the border router to be used as the next hop to the networks listed in the IBM 6611's updates to the BGP group.

The IBM 6611 can advertise any internal (belongs to the same autonomous system as the IBM 6611) or external (belongs to a different autonomous system) border router as the next hop, provided that the network portion of the IP address of the border router shares a common subnet with both the IBM 6611 and the BGP group.

Required: No

Dependencies: If an "Interface IP Address" on page 3-71 for the BGP group is specified, the subnet address portion of the Next hop destination must match the subnet address portion of the Interface IP address for the BGP group.

If an Interface IP address is **not** specified, the subnet address portion of the Next hop destination must match the subnet address portion of an interface on the IBM 6611.

Valid Values: Any IP address defined for the IBM 6611 in which the host portion of the address is non-zero

Default Value: None

Interface IP Address: This parameter specifies the IP address of the interface on the IBM 6611 to use when connecting to the neighbors in the BGP group. (See “BGP Group Type” on page 3-69.)

This parameter can be used for all group types, but is most useful for IGP group types. Because the IBM 6611 cannot automatically determine which of its addresses is the interface, it is recommended that this parameter be used for IGP group types.

Required: No

Dependencies: The IP address must be defined for an interface on the IBM 6611.

Valid Values: Any IP address defined for the IBM 6611

Default Value: None

Generate Default Route:

Disabling this parameter specifies that the internal default route will *not* be used for routing information learned from the BGP group.

Enabling this parameter specifies that BGP will use the setting of “Generate Default Route” on page 3-68.

Dependencies: This parameter overrides “Generate Default Route” on page 3-68, if that parameter is set to **Enable**.

Note: If “Generate Default Route” on page 3-68 is set to **Disable**, this parameter is not selectable.

Required: No

Valid Values: Enable, Disable

Default Value: Enable

Default Network In: This parameter controls whether the default network (0.0.0.0) can be imported in updates exchanged with the BGP group.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Passive: This parameter specifies that active opens to the BGP group should not be attempted. Enabling this parameter prevents closing of the connection to the BGP group when traffic is not being passed across the link.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Default Network Out: This parameter controls whether the default network (0.0.0.0) can be exported in updates exchanged with the BGP group.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Preference (0 – 255): This parameter specifies the preference value for routes that are learned from any BGP configured or unconfigured neighbor in the BGP group. If a value is not specified, BGP uses a value of 150.

The preference value is used to determine which route to use when multiple routes to the same destination exist. The route with the lowest preference value is used.

Note: This parameter is ignored for BGP group types IGP and test. (See “BGP Group Type” on page 3-69.)

Required: No

Dependencies: If you specify a value for this parameter, it will override any value you specify for “Default Preference (0 – 255)” on page 3-68.

Valid Values: 0 to 255 (with the lowest value being the most preferred)

Default Value: None

Hold Time: This parameter specifies the maximum number of seconds that can elapse between the receipt of successive keepalive, update, or notification messages before the connection will be closed. If a hold time is not specified, BGP will use a value of 180.

Required: No

Dependencies: None

Valid Values: 20 to 65535

Default Value: None

BGP Neighbor Parameters

The BGP neighbor parameters are specified for each BGP neighbor that is defined. At least one BGP neighbor (configured or unconfigured) must be defined per BGP group.

Note: BGP neighbor parameter values override BGP group parameter values.

Configured Neighbor Parameters

BGP Neighbor IP Address: This parameter specifies the IP address of the BGP configured neighbor.

Required: Yes

Dependencies: None.

Valid Values: A valid IP address. The host portion of the address must be non-zero.

Default Value: None

BGP Neighbor Name: This parameter specifies the user-defined name that identifies the BGP neighbor.

Required: No

Dependencies: None

Valid Values: Any alphanumeric value from 1 to 16 digits in length

Default Value: None

Metric Out: This parameter specifies the default metric given by the IBM 6611 to all routes propagated to the BGP neighbor. This parameter is ignored for IGP neighbors.

This parameter overrides "Metric Out" on page 3-70.

Required: No

Dependencies: This parameter cannot be specified if the configured neighbor is in an internal BGP group. (See "BGP Group Type" on page 3-69.)

Valid Values: 0 to 65535

Default Value: None

Next Hop Destination: This parameter specifies the IP address of the border router to be used as the next hop to the networks listed in the IBM 6611's updates to the neighbor.

The IBM 6611 can advertise any internal (belongs to the same autonomous system as the IBM 6611) or external (belongs to a different autonomous system) border router as the next hop, provided that the network portion of the IP address of the border router shares a common subnet with both the IBM 6611 and the configured neighbor.

This parameter overrides the "Next Hop Destination" on page 3-70.

Dependencies: If an "Interface IP Address" for the configured neighbor is specified, the subnet address portion of the Next hop destination must match the subnet address portion of the "Interface IP Address" for the configured neighbor.

If an "Interface IP Address" on page 3-71 for the BGP group of the configured neighbor is specified, (and **no** is specified for the "Interface IP Address" for the configured neighbor), the subnet address portion of the Next hop destination must match the subnet address portion of the "Interface IP Address" for the BGP group.

If **no** is specified for interface IP address, the subnet address portion of the Next hop destination must match the subnet address portion of an interface on the IBM 6611.

Required: No

Valid Values: Any IP address defined for the IBM 6611 in which the host portion of the address is non-zero

Default Value: None

Interface IP Address: This parameter specifies the IP address of an interface on the IBM 6611 over which to connect to the BGP configured neighbor. It is recommended that this parameter always be used for IGP group types because the IBM 6611 cannot automatically determine which of its local addresses is the interface over which to connect.

This parameter cannot be specified if the configured neighbor is in an internal BGP group. (See "BGP Group Type" on page 3-69.)

Required: No

Dependencies: The IP address must be defined for an interface on the IBM 6611.

This parameter overrides "Interface IP Address" on page 3-71 for the neighbor's BGP group.

Valid Values: An IP address configured for the IBM 6611.

Default Value: None

Generate Default Route:

Disabling this parameter specifies that the internal default route will **not** be used for routing information learned from the BGP configured neighbor.

Enabling this parameter specifies that BGP will use the setting of "Generate Default Route" on page 3-68.

Required: No

Dependencies: This parameter overrides "Generate Default Route" on page 3-68, if that parameter is set to **Enable**.

Note: If "Generate Default Route" on page 3-68 is set to **Disable**, this parameter is not selectable.

Valid Values: Enable, Disable

Default Value: Enable

Default Network In: This parameter controls whether the default network (0.0.0.0) can be imported in updates exchanged with the BGP configured neighbor.

This parameter overrides the setting of “Default Network In” on page 3-71 for the neighbor’s BGP group.

Required: No

Dependencies This parameter cannot be selected if the neighbor is in an internal BGP group. (See “BGP Group Type” on page 3-69.)

Valid Values: Enable, Disable

Default Value: Disable

Passive: This parameter specifies that active opens to the BGP configured neighbor should not be attempted. Enabling this parameter prevents closing of the connection to the BGP configured neighbor when traffic is not being passed across the link.

This parameter overrides “Passive” on page 3-71 for the configured neighbor’s BGP group.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Default Network Out: This parameter controls whether the default network (0.0.0.0) can be exported in updates exchanged with the BGP configured neighbor.

This parameter overrides “Default Network Out” on page 3-72 for the configured neighbor’s BGP group.

Required: No

Dependencies: This parameter cannot be selected if the neighbor is in an internal BGP group. (See “BGP Group Type” on page 3-69.)

Valid Values: Enable, Disable

Default Value: Disable

Preference (0 – 255): This parameter specifies the preference value for routes that are learned from the BGP configured neighbor. If a value is not specified, BGP uses a value of 150.

The preference value is used to determine which route to use when multiple routes to the same destination exist. The route with the lowest preference value is used.

Note: This option is ignored for BGP group types IGP and test.

Required: No

Dependencies: This parameter overrides “Preference (0 – 255)” on page 3-72 for this neighbor’s BGP group.

Valid Values: 0 to 255 (with the lowest values being the most preferred)

Default Value: None

Hold Time: This parameter specifies the maximum number of seconds that can elapse between receipt of successive keepalive, update, or notification messages before the connection will be closed. If no hold time is specified, BGP uses a value of 180.

Required: No

Dependencies: This parameter overrides “Hold Time” on page 3-72 for the configured neighbor’s BGP group.

Valid Values: 20 to 65535

Default Value: None

Unconfigured Neighbor Parameters

Neighbor: This parameter specifies an unconfigured neighbor to which the IBM 6611 will allow a BGP connection. The IBM 6611 allows unconfigured neighbors to connect if:

- An appropriate “BGP Group Type” on page 3-69 has been specified, with authentication done by address and mask checking against the unconfigured neighbor’s IP address.
- The unconfigured neighbor originates the request.

Although this parameter can be used by any BGP group, it is especially useful if you want to:

- Use an internal group to bring up internal BGP neighbors without reconfiguring the IBM 6611
- Use a test group to let a variety of testers connect.

The IBM 6611 will not try to connect to an unconfigured neighbor; however, it will allow a BGP connection with an unconfigured neighbor if the unconfigured neighbor initiates the connection and has specified the IBM 6611 as a configured neighbor.

Required: No

Dependencies: None

Valid Values

All Any neighbor running BGP that tries to connect to the IBM 6611.

Host A specific neighbor running BGP. Any host as specified by its IP address is allowed.

Network Any network as specified by its IP address.

Default Value: All

IP Address: This parameter specifies the IP address of a BGP unconfigured neighbor.

Required: Yes (if the “Neighbor” is specified as a Host or Network)

Dependencies: None

Valid Values

Host A valid IP address with non-zeros for the host portion of the address.

Network The default network (0.0.0.0.) or a valid IP address with zeros for the host portion of the address.

Default Value: None

BGP Neighbor Name: This parameter specifies the user-defined name that identifies a BGP neighbor.

Required: No

Dependencies: None

Valid Values: Any alphanumeric from 1 to 16 digits in length

Default Value: None

Mask: This parameter specifies the mask that identifies the selected **Network** unconfigured neighbors to which the IBM 6611 can communicate. (See “Neighbor” on page 3-76.)

Required: No

Dependencies: This parameter is required if a subnet address is specified. (See “IP Address” on page 3-76.)

Valid Values: Any mask as specified by its dotted-decimal notation

Default Value: None

BGP Import Filters

The BGP import filter parameters are specified for each autonomous system from which routes are to be imported.

Enable BGP Import Filters: This parameter specifies whether BGP imports are enabled or disabled for the IBM 6611.

- If this parameter is set to **Enable**, no routes are imported except those specified by one or more of the following parameters
 - Autonomous system number
 - AS path
 - Destination.
- If this parameter is set to **Disable**, no import filtering is done by BGP and all BGP routes are imported.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

List of BGP Imports

The following parameters, when specified, create a list of BGP import specifications for each autonomous system or autonomous system path from which routes will be imported.

Import Route Filters: This parameter specifies whether the import specifications apply to an autonomous system or autonomous system path.

- If **AS number** is selected, “Autonomous System Number” and “BGP Import Name” are required.
- If **AS path** is selected, “BGP Import Name,” “Autonomous System Path Specification,” and “AS Path Origin” on page 3-80 are required.

Required: No

Dependencies: None

Valid Values: AS number, AS path

Default Value: AS number

BGP Import Name: This parameter specifies a user-defined name for a BGP import.

Required: Yes

Dependencies: None

Valid Values: Any alphanumeric from 1 to 16 digits in length

Default Value: None

Autonomous System Number: This parameter specifies the autonomous system to which the import specifications for a destination apply.

This parameter is specified only once for each unique destination from which routes are imported.

Required: Yes (if **AS number** is selected for “Import Route Filters”)

Dependencies: None

Valid Values: 1 to 65534

Default Value: None

Autonomous System Path Specification: This parameter is used to identify one or more autonomous system paths to which you wish to apply import route filters.

Because certain autonomous system path constructs occur frequently, the following notational shorthand has been implemented to make autonomous system path specification easier. You may wish to use the following applicable symbols to specify the autonomous system path. (Refer to RFC 1164.)

.	Matches any autonomous system number.
	A regular expression followed by * means zero or more repetitions .
+	A regular expression followed by + means one or more repetitions .
?	A regular expression followed by ? means zero or one repetition .
	Alternation.
()	Parentheses group subexpressions. An operator, such as * or +, can stand for a single element or an expression that is enclosed in parentheses.
{m,n}	A regular expression followed by {m,n} (where m and n are both non-negative integers and m is less than or equal to n) means at least m and at most n repetitions .
{m}	A regular expression followed by {m} means exactly m repetitions .
{m,}	A regular expression followed by {m,} means m or more repetitions .

Autonomous System Path Specification Examples:

The following examples provide:

- Interpretations of autonomous system path specifications
- Specific autonomous system paths that match and do not match the autonomous system path specifications.

Example 1: (91 | 3) .*

This expression states that routing information coming from either Autonomous System 91 or Autonomous System 3 matches the autonomous system path specification. This includes routes from autonomous systems that lie beyond Autonomous System 91 and Autonomous System 3.

The following paths match the Example 1 autonomous system path specification:

91 5 73 6 9
91
91 44 8 67
91 44 8
3
3 7 78 32 2 20

The following paths do **not** match the Example 1 autonomous system path specification:

4 91 55 22 72
99 91
7 78 32 2 20
7 3 41

Example 2: (4 | 5)

This expression matches only routes that are received from Autonomous System 4 and Autonomous System 5 if Autonomous System 4 and Autonomous System 5 are adjacent to the IBM 6611's autonomous system.

The following paths match the Example 2 autonomous system path specification:

5
4

The following paths do **not** match the Example 2 autonomous system path specification:

4 5
4 1 7
5 78 9
8 5
8 22 49

Example 3: 2 .*

This expression matches any path coming from or through Autonomous System 2 if Autonomous System 2 is adjacent to the IBM 6611's autonomous system.

Example 4: 3 2 .*

This expression matches any path coming from Autonomous System 3 if the previous autonomous system in the path was Autonomous System 2 and Autonomous System 3 is adjacent to the IBM 6611's autonomous system.

Example 5: .* 3 2 .*

This expression matches any path with Autonomous System 3 followed immediately by Autonomous System 2.

The following paths match the Example 5 autonomous system path specification:

3 2 7 9
88 40 3 2
88 40 3 2 95

The following paths do **not** match the Example 5 autonomous system path specification:

3 1 2 5
88 40
88 40 2 95
63 3 6 2

Required: Yes (if **AS path** is selected for "Import Route Filters" on page 3-78)

Dependencies: None

Valid Values: From 1 to 80 integers and notational shorthand symbols as detailed in the description of this parameter.

Default Value: None

AS Path Origin: This parameter defines the origin of the path information specified for the "Autonomous System Path Specification" on page 3-78. In other words, the AS path origin indicates how a particular route was injected into BGP (for example, by the Exterior Gateway Protocol [EGP], an Interior Gateway Protocol [IGP], or some other means).

- If **IGP** is selected, BGP will import destinations that were learned by BGP from an IGP, such as OSPF.
- If **EGP** is selected, BGP will import destinations that were learned by BGP from EGP.
- If **Incomplete** is selected, BGP will import destinations that were learned by BGP by some other means (for example, from static route information).

- If **Any** is selected, BGP will import destinations that were learned by BGP from any of the above three origins.

Required: Yes (if **AS path** is selected for “Import Route Filters” on page 3-78)

Dependencies: None

Valid Values: IGP, EGP, Incomplete, Any

Default Value: Any

Restrict Imports: If this parameter is set to **Enable**, all routes associated with the “BGP Import Name” on page 3-78 and either the “Autonomous System Number” on page 3-78 or “Autonomous System Path Specification” on page 3-78 will **not** be imported.

Required: No

Dependencies: If a value is specified for “Preference (0 – 255),” and, then, this parameter is set to **Enable**, the preference value will be ignored.

Valid Values: Enable, Disable

Default Value: Disable

Preference (0 – 255): This parameter defines the default preference assigned to all BGP routes that are imported. If a value is not specified, BGP uses a value of 150.

Required: No

Dependencies: None

Valid Values: 0 to 255 (with the lowest values being the most preferred).

Default Value: None

Destination: This parameter specifies the destination that should be filtered. Either a destination IP address for each BGP route to be imported, or the word **all** must be specified.

If a finite number of destinations are to be restricted, the word **ALL** can be used in combination with “Restrict Routes” on page 3-82 to restrict some, but not all, routes from being imported. To do this:

1. Set the BGP import filters parameter on the BGP Imports panel to **Enable**, if you have not already done so.
2. On the BGP Import Destination Detail panel:
 - a. Type **all** in the Destination field.
 - b. Press **Apply**. The word **ALL** will appear in the List of BGP Destinations window on the BGP Import Detail panel.
 - c. Set Restrict routes to **Enable**.
 - d. For each route you do *not* want imported, type the IP address in the Destination field and press **Apply**.

A list containing the word ALL and each IP address will be created in the List of BGP Destinations window.

Required: Yes

Dependencies: This parameter must be specified for each BGP import destination to be matched to the BGP routes imported. If “Restrict Imports” on page 3-81 is set to **Enable**, a value cannot be specified for this parameter.

Valid Values: A valid IP address or the word **all**.

Default Value: None

Destination Mask: This parameter defines the mask that will be applied to the “Destination” on page 3-81 for defining a range of IP addresses to be imported.

Required: No

Dependencies: If “Restrict Imports” on page 3-81 is set to **Enable**, a value cannot be specified for this parameter.

Valid Values: A valid IP address mask

Default Value: 255.255.255.255

Restrict Routes: Enabling this parameter restricts the routes that are specified by the “Destination” on page 3-81 and “Destination Mask” from being learned by BGP.

Required: No

Dependencies: If “Restrict Imports” on page 3-81 is set to **Enable**, this parameter cannot be set to **Enable**.

Valid Values: Enable, Disable

Default Value: Disable

Preference (0 – 255): This parameter defines the preference to be attached to the BGP routes that are imported. The preference value is used to determine which route to use when more than one route is available to the same destination.

The lowest value will be the most preferred.

Required: No

Dependencies: If “Restrict Imports” on page 3-81 is set to **Enable**, a value cannot be specified for this parameter. (See “Restrict Imports” on page 3-81.)

Valid Values: 0 to 255

Default Value: None

Exterior Gateway Protocol (EGP)

Use the worksheet on page A-11.

Enable Exterior Gateway Protocol (EGP): This parameter enables or disables EGP.

Required: No

Dependencies: When EGP is enabled, "Local Autonomous System Number," "EGP Group Name" on page 3-84, and "EGP Neighbor IP Address" on page 3-84 are required.

Valid Values: Enable, Disable

Default Value: Disable

Local Autonomous System Number: This parameter defines the autonomous system number for this IBM 6611.

Required: No

Dependencies: None

Valid Values: 1 to 65534

Default Value: None

Maximum Initial Packet Size: This parameter specifies the size of the largest EGP packet that is initially accepted or sent.

Required: No

Dependencies: None

Valid Values: 1024 to 65535 bytes

Default Value: 8192 bytes

Preference: This parameter defines the preference value for routes learned by EGP. This value is used to determine the route to use when routes learned from multiple protocols exist to the same destination. Zero indicates the most preferred route.

Required: No

Dependencies: None

Valid Values: 0 to 255

Default Value: 200

Generate Default Route: This parameter generates a default route pointing to this router. This route can be exported to other routers using the protocol default.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Default Metric: This parameter defines the default metric for routes used to send out EGP updates.

Required: No

Dependencies: None

Valid Values: 0 to 255

Default Value: 255

List of EGP Groups

EGP Group Name: This parameter is a user-defined name that is an identifier for each EGP neighbor group.

Required: Yes

Dependencies: This parameter is required to define the EGP group name.

Valid Values: Any alphanumeric character

Default Value: Default neighbor group

Neighbor ASN: This parameter identifies the autonomous system (AS). associated with the EGP neighbor group being defined. This value verifies that the incoming packets are from the AS.

Required: No

Dependencies: None

Valid Values: 1 to 65534

Default Value: None

Maximum Active Neighbors: This parameter defines the maximum number of EGP neighbors in this group which remain active at one time.

Required: No

Dependencies: None

Valid Values: 1 to the maximum number of defined neighbors

Default Value: None

List of EGP Neighbors

EGP Neighbor IP Address: This parameter is the IP address of a remote router or host that is defined as an EGP neighbor within this EGP group. This IBM 6611 exchanges EGP information such as Hello and polling packets with every EGP neighbor that is defined and running.

Required: Yes

Dependencies: None

Valid Values: A valid IP address

Default Value: None

Generate Default Routes from This Neighbor: This parameter advertises the default route to this router. This route can be exported to other protocols using the special protocol default.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Import Default Route: This parameter tells EGP whether or not to import the default route (0.0.0.0) when advertised by other routers. A *default route* determines where a router sends a packet when there is not a specific next hop to the packet's destination.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Export Default Route: This parameter tells EGP whether or not to export the default route (0.0.0.0) when making advertisements to other routers. A router uses the export default route when it sends a packet and there is no declared specific next hop to the packet's destination.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Minimum Hello Interval: This parameter defines the minimum time between sending hello packets to the EGP neighbor defined in this group. This parameter allows control over the frequency of checks for reachability.

Required: No

Dependencies: None

Valid Values: 30 to 900 seconds

Default Value: 30 seconds

Minimum Polling Interval: This parameter defines the minimum period of time between polls. The purpose of these polls is to collect routing update information.

Required: No

Dependencies: None

Valid Values: 120 to 3600 seconds

Default Value: 120 seconds

Default Metric: This parameter defines the metric for routes that are being sent to the EGP neighbor.

Required: No

Dependencies: This parameter overrides "Default Metric."

Valid Values: 0 to 255

Default Value: The value of "Default Metric"

EGP Group Options

Preference: This parameter defines the preference value for routes learned by EGP. This value is used to determine which route to use when multiple protocols learn that routes to the same destination exist. In such instances, the route with the lowest preference value is used.

Required: No

Dependencies: This parameter overrides the value of the preference set on the main EGP window.

Valid Values: 0 to 255

Default Value: 200

Default Metric: This parameter defines the metric for routes that are sent to the EGP neighbor.

Required: No

Dependencies: None

Valid Values: 0 to 255

Default Value: This parameter overrides the value of "Default Metric" which is configured on the main EGP window of the Configuration Program.

Generate Default from This Neighbor Group: This parameter defines the default route generated for this neighbor group.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Import Default Route: This parameter tells EGP whether or not to import the default route (0.0.0.0) when received in advertisements from other routers.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Export Default Route: This parameter tells EGP whether or not to export the default route (0.0.0.0) when making advertisements to the routers. A router uses the export default route when it sends a packet and there is no declared specific next hop to the packet's destination.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Minimum Hello Interval: This parameter defines the minimum time between the sending of Hello packets to the EGP neighbor defined in this group.

Required: No

Dependencies: None

Valid Values: 30 to 900 seconds

Default Value: 30 seconds

Minimum Polling Interval: This parameter defines the minimum period of time between polls that this router takes of the EGP neighbors defined in this group.

Required: No

Dependencies: None

Valid Values: 120 to 3600 seconds

Default Value: 120 seconds

Next Hop Address or Domain Name: This parameter defines the address of a router on an attached network that provides the next hop destination to an EGP peer that is not on any attached network of this router.

Required: No

Dependencies: If all of the EGP peers in this group are on an attached network, this parameter is not required.

Valid Values: IP Address or Domain Name

Default Value: None

EGP Imports

Enable EGP Import Filters: This parameter enables or disables all EGP import filters.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

List of EGP Imports

Autonomous System Number: This parameter specifies the autonomous system number to which the imports specifications apply.

Required: Yes

Dependencies: This parameter is required to define a list of EGP imports.

Valid Values: 1 to 65534

Default Value: None

Restrict: When this parameter is set **Enable**, all EGP routes that are defined by an IP address and mask are not imported. When this parameter is set to **Disable**, all EGP routes are imported.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Preference: This parameter defines the preference attached to all EGP routes that are imported. Zero indicates the most preferred route.

Required: No

Dependencies: None

Valid Values: 0 to 255

Default Value: 200

List of EGP Import Destinations

These parameters are configured for each destination.

Destination: This parameter defines the IP address of the destination that matches the destination in the EGP route that is imported.

Required: Yes

Dependencies: This parameter is required to define EGP import destinations.

Valid Values: A valid IP address

Default Value: None

Destination Mask: This parameter defines the mask which is applied to the IP address that defines a range of IP addresses that are imported.

Required: No

Dependencies: None

Valid Values: A valid IP address mask

Default Value: 255.255.255.255

Restrict Routes: This parameter defines when the routes defined by the destination IP address and mask are restricted from being added to the local route table.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Preference: This parameter defines the preference attached to EGP routes that are imported. The preference value is used to determine the route to use when more than one route is available to the same destination.

Required: No

Dependencies: None

Valid Values: 0 to 255

Default Value: 200

Static Routes

Use the worksheet on page A-12.

The purpose of defining static routes is to define a communication path between networks that the network administrators believe to be commonly used and most operational.

A static route is defined by a pair of IP addresses. One address is the address of a router on a network that is attached to this IBM 6611. Sometimes this address is referred to as the *next hop*. The IBM 6611 allows you to define three **next hop routers**. The other IP address in the pair is the destination address of the route. This address identifies either a network or host. A network address can be easily recognized because the host value is zero.

After a static route is defined, it is added to the route table of the IBM 6611.

Restrictions: The IBM 6611 maintains only one route to a destination per protocol per AS. When there are multiple protocols with routes to the same destination, the route provided by the protocol with the lowest route preference is selected. If the route preferences are equal, then the route with the lowest AS number is selected. If the autonomous systems are equal, then the route with the lowest numeric next-hop gateway is selected.

List of IP Static Routes

Destination Address: This parameter defines the destination network or destination host for this static route.

Required: Yes

Dependencies: This parameter is required to define a static route.

Valid Values: A valid IP address

Default Value: None

Destination Mask: This parameter defines the mask that is applied to the IP address to define a range of IP addresses that match this destination.

Required: No

Dependencies: None

Valid Values: A valid IP address mask

Default Value: 255.255.255.255

Next Hop Router #1: This parameter defines the IP address of a router on an attached network that is the next hop router.

Required: Yes

Dependencies: This parameter is required to define a static route.

Valid Values: A valid IP address

Default Value: None

Next Hop Router #2: This parameter defines the IP address of a router on an attached network that is the next hop router.

Required: Yes

Dependencies: This parameter is required to define a static route.

Valid Values: A valid IP address

Default Value: None

Next Hop Router #3: This parameter defines the IP address of a router on an attached network that is the next hop router.

Required: Yes

Dependencies: This parameter is required to define a static route.

Valid Values: A valid IP address

Default Value: None

Preference: This parameter defines the route preference for this static route. The route preference determines the route to use by selecting the route from the protocol with the lowest preference among different routes to the same destination.

Required: No

Dependencies: None

Valid Values: 0 to 255

Default Value: 50

Retain Route in Master Table: This parameter causes a route to be retained in the system's master routing table when the IP routing protocols are shut down.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Packet Filters

Use the worksheet on page A-12.

Packet filters permit or deny specified traffic passing through the IBM 6611. The filters operate in a linear sequence based on the ID, reflecting the order in which the filtration occurs. For example, when you want to accept only one address from a specific network, you must add a filter with one filter ID to permit traffic from the specific network address, and then, add a filter with a higher filter ID to deny all other traffic from that network. The singular filter can be for a specific host address, an entire subnetwork, an entire network, all traffic, or combinations. It applies to source and destination addresses. Dual filters allow traffic to flow or not flow between two specific hosts, subnetworks, networks, or combinations of the three. To specify the device to be filtered, an address and a filter mask must be used. You should understand how subnet masking works to determine a filter's coverage.

Wherever the mask contains a zero, for example 0.0.0.0, all traffic can be permitted or denied. However, for a mask of 255.255.255.255, all address bits are significant, and the filter applies to a single address or host. Here are some examples:

IP Address = 9.67.2.2; Filter Mask = 255.0.0.0
Therefore, filters all traffic from network 9.0.0.0

IP Address = 9.67.2.2; Filter Mask = 255.255.0.0
Therefore, filters all traffic from subnetwork 9.67.0.0

IP Address = 9.67.2.2; Filter Mask = 0.0.0.0
Therefore, filters all traffic from all hosts.

Note: These filter masks do not have to line up with the subnet masks used for routing. (For example, you can use a subnet mask of 255.255.0.0 for class A in a network using 9.0.0.0, and you can enter a filter with the IP address of 9.67.2.2 and the filter mask is 255.254.0.0.) This combination would filter out subnets 9.67 and 9.66.

Filters affect the throughput capabilities of the IBM 6611. Therefore, filter arrays must be concise. Dual filters should be added to the end of the list when possible.

Status of All Defined IP Filters: This parameter enables or disables all IP filters that are configured. If IP filters are not configured, this parameter does not affect configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

List of IP Packet Filters

IP Filter ID: The filter ID is a decimal number. The number must be selected according to how the sequence of the incoming traffic is filtered. A filter with a lower ID number is enabled before a filter with a higher ID number. For example, when you want to permit a specific host access but deny access to the rest of the network, the permit filter (in this case the host) must have a lower ID number than the deny filter number (in this case the network). Otherwise, the deny removes all traffic from that network including the host to which you want to permit access.

Required: Yes

Dependencies: None

Valid Values: 1 to 100

Default Value: The next unused ID number

Filter Type: This parameter defines the type of filter for a specific ID. When this filter is set to **Singular**, it identifies a host, a subnet, a network, all hosts, or a combination with a single expression. When this filter is set to **Dual**, the filter identifies two end points from which to deny or allow traffic.

Singular Filters Filter all traffic to and from a specified entity. That is, traffic where the entity is the source that is filtered and traffic where the entity is the destination that is filtered.

Dual Filters Have a direction implied. Meaning, only traffic that is sourced was filter address and mask 1, and traffic that is destined to filter address and mask 2 will be filtered. To limit two entities from communicating with each other through the IBM 6611, two dual filters must be used.

Required: No

Dependencies: None

Valid Values: Singular, Dual

Default Value: Singular

Permit or Deny Traffic: This parameter specifies whether the traffic for a specific ID is to be permitted through the IBM 6611 or is to be discarded.

Required: No

Dependencies: None

Valid Values: Permit, Deny

Default Value: Permit

Filter IP Address 1: This parameter specifies the address of the host, subnetwork, or network for a specific filter ID. For dual filters, this is one of the end points, the source end point. For singular filters, this is the only end point.

Required: Yes

Dependencies: None

Valid Values: 0.0.0.0 to 255.255.255.255

Default Value: None

Filter Subnet Mask 1: This parameter specifies the mask for a specific filter ID. The mask, along with the IP address, dictates the range of addresses to be filtered.

Required: No

Dependencies: None

Valid Values: 0.0.0.0 to 255.255.255.255

Default Value: None

Filter IP Address 2: This parameter specifies the destination address of the host, subnetwork, or network for a specific filter ID. This address is used to check the destination parameter in the packet. This parameter applies only to dual filters. (See "Filter Type" on page 3-93)

Required: No

Dependencies: This parameter applies to dual filters only.

Valid Values: 0.0.0.0 to 255.255.255.255

Default Value: None

Filter Subnet Mask 2: This parameter specifies the mask for a specific filter ID. The mask along with the IP address dictates the range of addresses to be filtered.

Required: No

Dependencies: This parameter applies to dual filters only.

Valid Values: 0.0.0.0 to 255.255.255.255

Default Value: None

Route Exports

Use the worksheet on page A-13.

These parameters are configured for each route export.

List of Exports

Export Selection Name: This parameter is the assigned name for the defined export selection.

Required: Yes

Dependencies: This parameter is required to define a list of exports.

Valid Values: A string of alphanumeric characters

Default Value: None

From Protocol: This parameter determines the protocol from which data is exported.

Required: No

Dependencies: None

Valid Values: EGP, RIP, HELLO, Static, Default, OSPF, OSPF ASE (autonomous system external link), Direct, BGP, AS PATH

Default Value: EGP

Export destination: This parameter defines the destination to export.

Required: Yes

Dependencies: This parameter is required when "Export Selection Name" is configured.

Valid Values: All, Network IP address, Host IP address

Default Value: None

AS Number: This parameter determines the autonomous system number from which to add exported routes.

Required: No

Dependencies: This parameter is required if **BGP** or **EGP** is selected for the "From Protocol" parameter.

Valid Values: 1 to 65536

Default Value: None

Destination Mask: This parameter defines the mask to be applied to the IP address in "Export destination."

Required: No

Dependencies: None

Valid Values: 0.0.0.0 to 255.255.255.255

Default Value: 255.255.255.255

Metric: This parameter defines the metric for an exported route.

Required: No

Dependencies: This parameter is required when “Export Selection Name” on page 3-95 is configured and “Restrict” is set to **Disable**.

Valid Values: A valid metric for an exported route.

RIP	1 to 16.
HELLO	100 to 30 000.
EGP	0 to 255.
OSPF	0 to 65 535.
BGP	0 to 65 535.

Default Value:

RIP	1
HELLO	100
EGP	1
OSPFASE	1
BGP	None
AS PATH	None.

Restrict: This parameter defines whether the routes defined in “Export destination” on page 3-95 and “Destination Mask” on page 3-95 are restricted or not restricted from being added to the local route table. The default (disable) ensures that the routes are not restricted.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Autonomous System Path Specification: This parameter is used to identify one or more autonomous system paths to which you wish to apply import route filters.

Because certain autonomous system path constructs occur frequently, the following notational shorthand has been implemented to make autonomous system path specification easier. You may wish to use the following applicable symbols to specify the autonomous system path. (Refer to RFC 1164.)

Matches any autonomous system number.

A regular expression followed by * means **zero or more repetitions**.

+	A regular expression followed by + means one or more repetitions .
?	A regular expression followed by ? means zero or one repetition .
	Alternation.
()	Parentheses group subexpressions. An operator, such as * or +, can stand for a single element or an expression that is enclosed in parentheses.
{m,n}	A regular expression followed by {m,n} (where m and n are both non-negative integers and m is less than or equal to n) means at least m and at most n repetitions .
{m}	A regular expression followed by {m} means exactly m repetitions .
{m,}	A regular expression followed by {m,} means m or more repetitions .

Autonomous System Path Specification Examples:

The following examples provide:

- Interpretations of autonomous system path specifications
- Specific autonomous system paths that match and do not match the autonomous system path specifications.

This expression states that routing information coming from either Autonomous System 91 or Autonomous System 3 matches the autonomous system path specification. This includes routes from autonomous systems that lie beyond Autonomous System 91 and Autonomous System 3.

The following paths match the Example 1 autonomous system path specification:

```
91 5 73 6 9
91
91 44 8 67
91 44 8
3
3 7 78 32 2 20
```

The following paths do **not** match the Example 1 autonomous system path specification:

```
4 91 55 22 72
99 91
7 78 32 2 20
7 3 41
```

Example 2: (4 | 5)

This expression matches only routes that are received from Autonomous System 4 and Autonomous System 5 if Autonomous System 4 and Autonomous System 5 are adjacent to the 6611's autonomous system.

The following paths match the Example 2 autonomous system path specification:

```
5
4
```

The following paths do **not** match the Example 2 autonomous system path specification:

4 5
4 1 7
5 78 9
8 5
8 22 49

This expression matches any path coming from or through Autonomous System 2 if Autonomous System 2 is adjacent to the IBM 6611's autonomous system.

This expression matches any path coming from Autonomous System 3 if the previous autonomous system in the path was Autonomous System 2 and Autonomous System 3 is adjacent to the IBM 6611's autonomous system.

This expression matches any path with Autonomous System 3 followed immediately by Autonomous System 2.

The following paths match the Example 5 autonomous system path specification:

3 2 7 9
88 40 3 2
88 40 3 2 95

The following paths do **not** match the Example 5 autonomous system path specification:

3 1 2 5
88 40
88 40 2 95
63 3 6 2

Required: Yes (if AS path is selected for the "From Protocol" on page 3-95 parameter)

Dependencies: None

Valid Values: From 1 to 80 integers and notational shorthand symbols as detailed in the description of this parameter.

Default Value: None

AS Path Origin: The AS path origin parameter defines the origin (IGP, EGP, Incomplete, or Any) of the path information defined for the "Autonomous System Path Specification" on page 3-96. In other words, the AS path origin indicates how a particular route is injected into BGP (for example, by the Exterior Gateway Protocol [EGP]), an Interior Gateway Protocol [IGP], or some other means).

If **IGP** is selected, BGP will import destinations that were learned by BGP from an IGP, such as OSPF.

If **EGP** is selected, BGP will import destinations that were learned by BGP from EGP.

If **Incomplete** is selected, BGP will import destinations that were learned by BGP by some other means (for example, from static route information).

If **Any** is selected, BGP will import destinations that were learned by BGP from any of the above three origins.

Required: Yes (if AS path is selected for the “From Protocol” on page 3-95 parameter)

Dependencies: None

Valid Values: IGP, EGP, Incomplete, Any

Default Value: Any

To Protocol: This parameter defines the protocol to which data is exported.

Required: No

Dependencies: None

Valid Values: RIP, HELLO, EGP, OSPFase (autonomous system external link), BGP

Default Value: RIP

AS Number: This parameter determines the autonomous system number to add to exported routes.

Required: No

Dependencies: This parameter is required if **BGP** or **EGP** is selected for the “To Protocol” parameter.

Valid Values: 1 to 65536

Default Value: None

Type: This parameter identifies the OSPF external link type to add to exported routes.

Required: No

Dependencies: This parameter is required when “To Protocol” is set to **OSPFase** (autonomous system external link).

Valid Values: 1, 2

Default Value: None

Tag: This parameter identifies the tag to be added to the exported route.

Required: No

Dependencies: This parameter is required when “To Protocol” is set to **OSPFase** (autonomous system external link).

Valid Values: 1 to 65536

Default Value: None

IP over X.25

Connection Decay Interval: This parameter defines the amount of time an X.25 SVC remains connected after the last IP session has closed. This parameter prevents the cost to reestablish a call if the remote end is contacted again within the value of this parameter.

This is also the amount of time before an inactive complete ARP entry is deleted.

Required: No

Dependencies: None

Valid Values: 1 to 20 minutes

Default Value: 10 minutes

AppleTalk

AppleTalk** is a network protocol developed by Apple Computer, Inc. The protocol interconnects network devices, which may be a mixture of Apple and non-Apple products. The IBM 6611 supports AppleTalk Phase 2, which extends the capabilities of the AppleTalk protocol to handle more complex networks and internets.

To configure AppleTalk Phase 2 on the IBM 6611, you need to:

- Select **System Configuration** on the main menu of the configuration program. The parameter "Enable AppleTalk" is one of the System Configuration options. Set this parameter to **Enable**. (This parameter appears in the worksheet on page A-16.)
- Define the AppleTalk protocol on each adapter port connected to an AppleTalk network. See "AppleTalk Port Parameters" on page 6-57 for a description of how to configure the AppleTalk ports on the IBM 6611.

The AppleTalk Phase 2 protocol can be configured on a Token-Ring Network 16/4 Adapter, Ethernet Adapter, EIA 422/449 Serial Adapter, or V.35/V.36 Serial Adapter. On a EIA 422/449 Serial Adapter or V.35/V.36 Serial Adapter, AppleTalk is an option when the adapter is configured to support Frame Relay or the Point-to-Point Protocol (PPP). For more information about the AppleTalk Phase 2 protocol and how it is implemented on the IBM 6611, refer to the *IBM 6611 Network Processor Introduction and Planning Guide*.

Enabling the AppleTalk Protocol

The following parameter is the only system configuration parameter for the AppleTalk Phase 2 protocol.

Enable AppleTalk: This parameter enables or disables the routing of AppleTalk packets on all ports configured to support AppleTalk. When this parameter is disabled (the default), no AppleTalk packets are routed by the IBM 6611.

Note: If this parameter is disabled, but bridging has been defined, the IBM 6611 will bridge AppleTalk packets.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Internet Packet Exchange (IPX)

Use the worksheet on page A-14.

The Internetwork Packet Exchange (IPX) is a variation of Xerox Networking Services (XNS) provided by Novell. One difference between the two is that IPX on 802.3 media uses a variant of IEEE 802.2 encapsulation and XNS uses Ethernet encapsulation. Another difference between XNS and IPX is that IPX provides a Service Access Protocol (SAP), which is used to advertise network services in an IPX internet.

Restriction: When you configure IPX and XNS, you cannot use the SAPs, which are X'E0' for IPX and X'80' for XNS, to route data link switching traffic.

Enable IPX Router: This parameter enables or disables all ports configured for IPX.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Split Horizon for RIP Filters: When **On** is selected, the route process does not send out RIP information over a particular network for the routes acquired over that network. When **Poison Reverse** is selected, the route process sends out all RIP information over a particular network but sets the metric to infinite for those routes acquired over that network. When **Off** is selected, the route process sends out RIP information for all routes over all configured IPX ports.

Required: No

Dependencies: None

Valid Values: On, Poison Reverse, Off

Default Value: On

IPX Service Advertisement Protocol (SAP) Filters

All SAP filters define a network or group of IPX networks that are denied permission to access a specific IPX server or group of servers of a server type. SAP filters are optional parameters. The following list of parameters are configured once for each SAP filter.

Status of All Defined SAP Filters: This parameters enables or disables all defined SAP filters. When SAP filters are not defined, this parameter does not affect configuration.

Required: No

Dependencies: This parameter must be configured for all SAP filters.

Valid Values: Enable, Disable

Default Value: Enable

Filtering Mode: This parameter defines the filtering action to be taken. When **Deny** is selected, all service advertisement protocol (SAP) requests and responses that match any SAP routing filter are ignored. When **Permit** is selected, all SAP requests and responses that do not match a SAP routing filter are ignored.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

List of SAP Filters

Filter ID: This parameter uniquely identifies this filter.

Required: Yes

Dependencies: This parameter must be configured for each SAP filter. It is required to define SAP filters.

Valid Values: 1 to 128

Default Value: None

Server Type: This parameter defines which servers are filtered.

Required: No

Dependencies: This parameter must be configured to define a SAP filter. When this parameter is set to **Enter server types**, "Type" is required.

Valid Values: All server types, Enter server types

Default Value: All server types

Type: This parameter is the type of IPX server to be filtered.

Required: No

Dependencies: This parameter is required when "Server Type" is set to **Enter server types**.

Valid Values: X'1' to X'FFFE'

Default Value: None

Network Number: This parameter defines the IPX network number.

Required: No

Dependencies: This parameter is required to define a SAP filter. When this parameter is set to **Enter network number**, "Network" on page 3-104 is required.

Valid Values: All networks, Enter network number

Default Value: All networks

Network: This parameter is the IPX network to be filtered.

Required: No

Dependencies: This parameter is required when "Network Number" on page 3-103 is set to **Enter network number**.

Valid Values: X'0000 0001' to X'FFFF FFFE'

Note: X'0000 0000' and X'FFFF FFFF' are reserved.

Default Value: None

Server Name: When **All servers** is selected, all servers are filtered. When **Enter server name** is selected, "Name" is required.

Required: No

Dependencies: This parameter is required when you are defining a SAP filter.

Valid Values: All servers, Enter server name

Default Value: All servers

Name: This parameter is the name of the IPX server to be filtered.

Required: Yes

Dependencies: This parameter is required when "Server Name" is set to **Enter server name**.

Valid Values: A string of 1 to 48 alphanumeric characters

Default Value: None

IPX Router RIP Filters

A maximum of 10 filters per port can be defined. Configuring IPX router RIP filters is not required.

Status of All Defined RIP Router Filters: This parameter enables or disables all defined RIP router filters. When RIP router filters are not defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Filtering Mode: This parameter defines the filtering action to be taken. When **Deny** is selected, all routing requests and responses matching any routing filter are ignored. When **Permit** is selected, all routing requests and responses that do not match a routing filter are ignored.

Required: No

Dependencies: This parameter must be configured for all IPX router RIP filters.

Valid Values: Deny, Permit

Default Value: Deny

List of IPX Router RIP Filters

Filter ID: This parameter uniquely identifies this filter.

Required: Yes

Dependencies: This parameter must be configured for each filter. This parameter is required to define IPX router RIP filters.

Valid Values: 1 to 128

Default Value: None

Network Numbers to Filter on: This parameter defines routing information about the IPX network number filtered on the interface in "Filter ID."

Required: No

Dependencies: When this parameter is set to **Enter network number**, "Network Number" is required.

Valid Values: Enter network number, All networks

Default Value: All networks

Network Number: This parameter provides the network number for the IPX network that is listed in "Network Numbers to Filter on."

Required: No

Dependencies: This parameter is required when "Network Numbers to Filter on" is set to **Enter network number**.

Valid Values: X'0000 0000' to X'FFFF FFFF'

Default Value: None

Host Address to Filter on: When **All hosts** is selected, all routers on a network defined in "Network Numbers to Filter on" and "Network Number" on page 3-105 and received on a port defined in "Filter ID" are filtered according to permit and deny in "Filtering Mode" on page 3-104.

Required: No

Dependencies: When this parameter is set to **Enter host address**, "Host Address" must be configured.

Valid Values: Enter host address, All hosts

Default Value: All hosts

Host Address: This parameter identifies routing information from this host that is filtered.

Required: No

Dependencies: When "Host Address to Filter on" on page 3-113 is set to **Enter host address**, this parameter is required.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

IPX RIP Inbound Filters

A maximum of 10 filters per port can be configured. IPX inbound RIP filter parameters are not required.

Status of All Defined Inbound RIP Filters: This parameter enables or disables all defined inbound RIP filters. When inbound RIP filters are not defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Filtering Mode: This parameter defines the filtering action to be taken. When **Deny** is selected, all routing requests or responses matching any routing filter are ignored. When **Permit** is selected, all routing requests or responses that do not match a routing filter are ignored.

Required: No

Dependencies: This parameter is configured once for all IPX inbound RIP filters.

Valid Values: Deny, Permit

Default Value: Deny

List of IPX RIP Inbound Filters

Filter ID: This parameter uniquely identifies this filter.

Required: Yes

Dependencies: This parameter must be configured for each filter. This parameter is required to define IPX inbound RIP filters.

Valid Values: 1 to 128

Default Value: None

Local IPX Network to Filter on: This parameter defines whether routing information for a network is filtered on all local interfaces configured for IPX or some interface that is selected from a list in the Configuration Program.

Required: Yes

Dependencies: This parameter is configured for each IPX inbound RIP filter. X'FFFF FFFF' means all local interfaces.

Valid Values: X'0000 0000' to X'FFFF FFFF'

Default Value: None

Network Numbers to Filter on: This parameter defines routing information about the IPX network number that is filtered on the interface identified in "Local IPX Network to Filter on" on page 3-106.

Required: No

Dependencies: When this parameter is set to **Enter network number**, "Network Number" is required.

Valid Values: Enter network number, All networks

Default Value: All networks

Network Number: This parameter defines the network number on which this IPX network is filtered.

Required: No

Dependencies: This parameter is required when "Network Numbers to Filter on" is set to **Enter network number**.

Valid Values: X'0000 0000' to X'FFFF FFFF'

Default Value: None

IPX RIP Outbound Filters

Status of All Defined Outbound RIP Filters: This parameter enables and disables all defined outbound RIP filters. When outbound RIP filters are not defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Filtering Mode: This parameter defines the filtering action to be taken. When **Deny** is selected, all routing requests or responses matching any routing filter are ignored. When **Permit** is selected, all routing requests or responses not matching any routing filter are ignored.

Required: No

Dependencies: This parameter is configured once for all IPX outbound RIP filters.

Valid Values: Deny, Permit

Default Value: Deny

List of IPX RIP Outbound Filters

A maximum of 10 filters per port can be configured. IPX outbound RIP filter parameters are not required.

Filter ID: This parameter uniquely identifies this filter.

Required: Yes

Dependencies: This parameter must be configured for each filter. This parameter is required to define the IPX outbound RIP filters.

Valid Values: 1 to 128

Default Value: None

Local IPX Network to Filter on: This parameter defines whether routing information for a network is filtered on all local interfaces configured for IPX or some interface that is selected out of a list from other configured IPX ports.

Required: Yes

Dependencies: Assume IPX is configured on one or more ports before trying to configure these filters. This parameter is required to define IPX outbound RIP filters. X'FFFF FFFF' means all local interfaces.

Valid Values: X'0000 0000' to X'FFFF FFFF'

Default Value: None

Network Numbers to Filter on: This parameter defines routing information about the IPX network number filtered on the interface in "Local IPX Network to Filter on."

Required: No

Dependencies: When this parameter is set to **Enter network number**, "Network Number" is required.

Valid Values: Enter network number, All networks

Default Value: All networks

Network Number: This parameter defines the network number on which this IPX network is filtered.

Required: No

Dependencies: This parameter is required when "Network Numbers to Filter on" is set to **Enter network number**.

Valid Values: X'0000 0000' to X'FFFF FFFF'

Default Value: None

Xerox Networking System (XNS)

Use the worksheet on page A-15.

The XNS protocol combines a set of internet protocols that provide data transfer service over LAN and WAN networks. XNS provides the packet routing for XNS hosts and networks similar to that which IP provides for IP hosts and networks. When the XNS packet is received at the IBM 6611 and the IBM 6611 is configured to run XNS over the same physical network, then the XNS routing protocol is used to route the packet to another physical network that is also configured to use XNS.

Restriction: When you configure IPX and XNS, you cannot use the SAPs, which are X'E0' for IPX and X'80' for XNS, to route data link switching traffic.

Enable XNS Router: When this parameter is set to **Enable**, XNS routing is enabled on all ports configured for XNS. When this parameter is set to **Disable**, routing cannot occur on all ports configured for XNS.

Required: No

Dependencies: This parameter must be set to **Enable** to transmit XNS packets.

Valid Values: Enable, Disable

Default Value: Disable

Split Horizon For RIP Filters: When **On** is selected, the route process does not send RIP information over a particular network for the routes acquired over that network. When **Poison Reverse** is selected, the route process sends out all RIP information over a particular network, but sets the metric to infinity for those routes acquired over that network. When **Off** is selected, the route process sends out RIP information for all routes over all configured XNS ports.

Required: No

Dependencies: None

Valid Values: On, Poison Reverse, Off

Default Value: On

XNS Inbound RIP Filters

Status of All Inbound RIP Filters: This parameter enables or disables all inbound RIP filters that are configured. When inbound RIP filters are not defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Filtering Mode: This parameter defines the filtering action to be taken. When **Deny** is selected, all routing requests and responses, matching any routing filter are ignored. When **Permit** is selected, all routing requests and responses that do not match any routing filter are ignored.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

List of XNS Inbound RIP Filters

Filter ID: This parameter uniquely identifies this filter.

Required: Yes

Dependencies: This parameter must be configured for each filter. This parameter is required to define XNS inbound RIP filters.

Valid Values: 1 to 128

Default Value: None

Local XNS Network to Filter on: This parameter defines whether routing information for a network is filtered on all local interfaces configured for XNS or some interface that is selected from the list window in the Configuration Program.

Required: Yes

Dependencies: XNS must be configured on one or more ports before trying to configure these filters. X'FFFF FFFF' means all local interfaces. This parameter is required to define XNS inbound RIP filters.

Valid Values: X'0000 0000' to X'FFFF FFFF'

Default Value: None

Network Numbers to Filter on: This parameter defines the routing information for the XNS network number that is filtered on the interface identified in "Local XNS Network to Filter on."

Required: No

Dependencies: When this parameter is set to **Enter network number**, then "Network Number" is required.

Valid Values: Enter network number, All networks

Default Value: All networks

Network Number: This parameter defines the network number on which this XNS network is filtered.

Required: No

Dependencies: This parameter is required when "Network Numbers to Filter on" is set to **Enter network number**.

Valid Values: X'0000 0001' to X'FFFF FFFE'

Note: X'0000 0000' and X'FFFF FFFF' are reserved.

Default Value: None

XNS Outbound RIP Filters

A maximum of 10 filters per port can be configured. These filter parameters are not required.

Status of All Outbound RIP Filters: This parameter enables or disables all outbound RIP filters configured. When outbound RIP filter are not configured, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Filtering Mode: This parameter defines the filtering action to be taken. When **Deny** is selected, all routing requests and responses, matching any routing filter are ignored. When **Permit** is selected, all routing requests and responses that do not match any routing filter are ignored.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

List of XNS Outbound RIP Filters

Filter ID: This parameter uniquely identifies this filter.

Required: Yes

Dependencies: This parameter must be configured for each filter. This parameter is required to define XNS outbound RIP filters.

Valid Values: 1 to 128

Default Value: None

Local XNS Network to Filter on: This parameter defines whether routing information for a network is filtered on all local interfaces configured for XNS or some interface that is selected out of the list.

Required: Yes

Dependencies: This parameter is required to define XNS outbound RIP filters. XNS must be configured on one or more ports before trying to configured these filters. X'FFFF FFFF' means all local interfaces.

Valid Values: X'0000 0000' to X'FFFF FFFF'

Default Value: None

Network Numbers to Filter on: This parameter defines the routing information for the XNS network number that is filtered on the interface identified in "Local XNS Network to Filter on" on page 3-111.

Required: No

Dependencies: When this parameter is set to **Enter network number**, then "Network Number" is required.

Valid Values: Enter network number, All networks

Default Value: All networks

Network Number: This parameter defines the network number on which this XNS network is filtered.

Required: Yes

Dependencies: This parameter is required when "Network Numbers to Filter on" is set to **Enter network number**.

Valid Values: X'0000 0000' to X'FFFF FFFF'

Default Value: None

XNS RIP Router Filters

A maximum of 128 filters can be configured. These parameters are not required.

Status of All RIP Router Filters: This parameter enables or disables all RIP router filters configured. When RIP router filters are not configured, this parameter has no effect.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Filtering Mode: This parameter defines the filtering action to be taken. When **Deny** is selected, all routing requests and responses that match any routing filter are ignored. When **Permit** is selected, all routing requests and responses that do not match any routing filter are ignored.

Required: No

Dependencies: This parameter is configured once for all filters.

Valid Values: Deny, Permit

Default Value: Deny

List of XNS Router RIP Filters

Filter ID: This parameter uniquely identifies this filter.

Required: Yes

Dependencies: This parameter must be configured for each filter. This parameter is required to define XNS router RIP filters.

Valid Values: 1 to 128

Default Value: None

Network Numbers to Filter on: This parameter defines the routing information about the XNS number that is filtered on the interface identified in "Filter ID."

Required: No

Dependencies: This parameter is required to define XNS router RIP filters.

Valid Values: Enter network number, All networks

Default Value: All networks

Network Number: This parameter defines the network number on which this XNS network is filtered.

Required: No

Dependencies: This parameter is required when "Network Numbers to Filter on" is set to **Enter network number**.

Valid Values: X'0000 0000' to X'FFFF FFFF'

Default Value: None

Host Address to Filter on: When **All hosts** is selected, all routers on a network defined in "Network Numbers to Filter on" and "Network Number" on page 3-113 and received on a port defined in "Filter ID" are filtered according to permit and deny "Filtering Mode" on page 3-112.

Required: No

Dependencies: When **Enter host address** is selected, "Host Address" is required.

Valid Values: Enter host address, All hosts

Default Value: All hosts

Host Address: This parameter identifies routing information from this host that is filtered.

Required: No

Dependencies: When "Host Address to Filter on" is set to **Enter host address**, this parameter is required.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

List of XNS Static Routes

Please see "Static Routes" on page 3-90 for information regarding static routes.

Destination Network Number: This parameter defines the destination network for this static route.

Required: Yes

Dependencies: None.

Valid Values: X'0000 0001' to X'FFFF FFFE'

Default Value: None

Destination Network Number Mask: This parameter defines the mask that is applied to the network number to define a range of network numbers that match this destination.

Required: No

Dependencies: None

Valid Values: X'0000 0001' to X'FFFF FFFE'

Default Value: X'FFFF FFFE'.

Network Number of Next Hop Router: This parameter defines the network number of a router on an attached network that is the next hop router.

Required: No

Dependencies: This parameter is required to define a static route.

Valid Values: X'0000 0001' to X'FFFF FFFE'

Default Value: None

Next Hop Router Host Address: This parameter defines the host address of a router on an attached network that is the next hop router.

Required: Yes

Dependencies: None

Valid Values: 12 hexadecimal digits

Default Value: None

DECnet

Use the worksheet on page A-17.

DECnet Phase IV protocol was developed by the Digital Equipment Corporation. A DECnet network is hierarchical and segmented into *areas*. Each unique area within the network is assigned a decimal value from 1 to 63. Within an area, nodes are identified as either a router or a host. Nodes reside uniquely within one area and are assigned decimal values from 1 to 1023. Therefore, the address of a host or router in a DECnet network is unique by referring to the area number followed by the node number. References to DECnet nodes are represented in a decimal format. For example, when the host is 60.1002, then the area number is 60 and the node number is 1002.

Router nodes can support one or both of the two levels defined as DECnet Phase IV routing. *Level 1 routing* means routing within a DECnet area. *Level 2 routing* means routing between different areas. Level 1 routers maintain routes to destination nodes within their area as well as the route to the nearest level 2 router. Level 2 routers maintain route tables to other level 2 routers and to nodes within their own area.

When a level 1 router receives a packet to a destination that is within its area, it routes it to that node. When a level 1 router receives a packet with a destination that is outside of its DECnet area, the router will forward the packet to a level 2 router in its area. The packet can then pass through multiple routers before reaching a level 2 router for the destination area. Typically, level 2 routers can also perform level 1 routing function within their own area.

Functions of the DECnet router include the ability to:

- Determine the location of the other routers and hosts
- Build a model of the network's topology
- Select the best route for a particular packet to follow
- Manage packet lifetime control
- Manage packet congestion control.

A DECnet router periodically transmits Hello and topology messages to determine the location and characteristics of the hosts and routers in the extended network. The information in these messages enables the IBM 6611 to develop the network's topology and to determine the best route to each node in the network. A DECnet router uses a connectivity algorithm to maintain lengths, and it uses a traffic assignment to maintain path costs. The information from these algorithms is used to update the routing database.

One attribute is assigned to a router per port priority. This value ranges from 0 to 127. Priority is used to define which router on a LAN segment is the designated router. The designated router on a physical segment within an area is selected as the one with the higher priority. If two routers have the same priority, then the router with the higher address is selected. A designated router performs the additional duties of informing the end nodes on the segment of the existence and identity of other routers. The designated router is the router designated to provide message routing services for end nodes on Ethernet and token-ring segments.

A DECnet router uses packet lifetime controls to limit the number of intermediate network nodes that a DECnet packet can pass through. This control prevents the effects of looping packets.

The DECnet protocol associates addresses with routers, not with adapter ports. The host, not the cable, has an identity. Therefore, a router can have only one DECnet address for each DECnet network of which it is a member.

Unlike other protocols, DECnet allows an area to span across many routers. A single cable can have many areas attached to it. Level 1 routing permits routing between multiple segments. Moreover, the hierarchical structure of DECnet allows level 2 routers to support multiple areas on a segment.

Restrictions: DECnet addressing specifies that every DECnet-enabled interface must have the same address.

DECnet Router Defaults

Enable DECnet Router: This parameter enables or disables DECnet routing on all ports configured for DECnet. When this parameter is set to **Disable**, DECnet cannot be routed on this IBM 6611.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Local DECnet Address: This parameter defines the DECnet address of an IBM 6611 node. This address is assigned to the IBM 6611. A DECnet MAC-level address is an encoded version of the 16-bit area and node combination. Every DECnet-enabled interface on the IBM 6611 must have the same MAC address.

Required: Yes

Dependencies: None

Valid Values: <area number>.<node number>

The *area number* is an integer ranging from 1 to 63. The *node number* is an integer ranging from 1 to 1023.

Default Value: None

Node Type: When **Routing IV** (Level 1) is selected, the IBM 6611 executes as a Level 1 router forwarding packets to destinations within the same area or to the closest DECnet area router within its area. When **Area** (Level 2) is selected, the DECnet router (referred to as an *area router*) performs Level 2 functions, forwarding packets to DECnet routers in other areas and to nodes within its own area.

Required: No

Dependencies: None

Valid Values: Routing IV, Area

Default Value: Routing IV

Area Maximum Hops: This parameter represents the maximum number of routing hops allowed between the local area router and any other area router in the network. A remote area is reachable if the total path cost and path length to the nearest area router in the remote area are less than the values specified for the “Area Maximum Cost” on page 3-117 and this parameter, respectively.

Required: No

Dependencies: This parameter is configured when “Node Type” on page 3-116 is set to **Area**.

Valid Values: 1 to 30

Default Value: 30

Area Maximum Cost: This parameter specifies the maximum total path cost between the local area (Level 2) router and any other area router in the network. A remote area is reachable when the total path cost and path length to the nearest area router in the remote area are less than the values specified for this and “Area Maximum Hops.”

Required: No

Dependencies: This parameter is valid only when “Node Type” is set to **Area**.

Valid Values: 1 to 1022

Default Value: 1022

Maximum Hops: This parameter represents the maximum number of routing hops allowed from the router to any other node within its own area. A hop is the logical distance of a circuit between two adjacent nodes. This parameter defines the point where the router declares another node unreachable because the length of the shortest path between the two nodes is too long.

Required: No

Dependencies: None

Valid Values: 1 to 30

Default Value: 30

Maximum Cost: This parameter represents the maximum path cost allowed from the IBM 6611 to any other node in its area. The path cost is the sum of the cost of each circuit cost along the path between two nodes. This parameter defines the point where the IBM 6611 declares that another node is unreachable because the cost of the least costly path to the other node exceeds this value.

Required: No

Dependencies: None

Valid Values: 1 to 1022

Default Value: 1022

Maximum Address: This parameter defines the largest node number and provides the maximum number of nodes that the DECnet router can detect within its area. All routers on the network should use the same values for this parameter.

Required: No

Dependencies: None

Valid Values: 1 to 1023

Default Value: 1023

Maximum Area: This parameter represents the largest area number within a network. It specifies the maximum number of areas in a DECnet network. Generally, all IBM 6611s on the network should use the same value for this parameter.

Required: No

Dependencies: None

Valid Values: 1 to 63

Default Value: 63

Maximum Visits: This parameter limits the maximum number of nodes through which a packet can be routed before arriving at its destination. This is the parameter that prevents packets from being endlessly looped through the network. If the number of nodes through which a packet passes exceeds the value of this parameter, the packet is discarded.

DEC recommends that the value of this parameter is at least twice that of "Maximum Hops" on page 3-117.

Required: No

Dependencies: None

Valid Values: 1 to 63

Default Value: 63

Maximum Broadcast Routers: This parameter sets the maximum number of routing nodes permitted on all Ethernet and token-ring networks to which the IBM 6611 is attached.

- On a Level 1 (Routing IV) router in a multiple area network, the parameter must be greater than or equal to the total number of routers (Level 1 and Level 2) in the same area on all segments to which the IBM 6611 is connected.
- On a Level 2 (Area) router, the parameter must be greater than or equal to the total number of all Level 1 and Level 2 routers in all the other areas on the connected LANs.

Required: No

Dependencies: None

Valid Values: 1 to 1022

Default Values: 32

Maximum Broadcast Non-Routers: This parameter defines the maximum number of non-routing nodes (end nodes) permitted on all Ethernet and token-ring networks to which the IBM 6611 is attached. The value of this parameter should be defined to be greater than or equal to the total number of end nodes on all Ethernet and token-ring networks connected to the IBM 6611. This total relates only to those end nodes within the same area as the IBM 6611. When two LANs are connected by a bridge, this parameter should be greater than or equal to all the end nodes in an entire extended LAN.

Required: No

Dependencies: None

Valid Values: 1 to 1022

Default Value: 1022

Routing Buffer Size: This parameter has two significant purposes:

- It determines the datalink block size that is advertised in the router Hello messages. The IBM 6611 has chosen to have the same datalink block size for all circuits.
- It also determines the maximum size DECnet phase IV packet (routing data or control) that would be received by the IBM 6611 software. It includes the routing headers and any pad bytes which might be prefixed to DECnet Phase-IV packets. It does not include the 2-byte byte-count field.

Note: IBM recommends that this parameter uses the default value.

Required: No

Dependencies: None

Valid Values: 246 to 1498 bytes

Default Value: 1498 bytes

DECnet Packet Filters

DECnet filters permit or deny specified traffic passing through the IBM 6611. The filters must be entered in a linear sequence of how the filtering is to occur. For example, when you want to deny all traffic from a specific area except for one node address, the filter ID of the filter to permit traffic from the specific node address should be lower than the filter ID of the filter which denies all traffic from the area. If there are no filter matches, the packet is permitted.

The singular filter can be applied to a specific DECnet node address, a subset of nodes belonging to an area, a subset of areas, or all traffic. The singular filter applies to both the source and destination address. Therefore, traffic is not permitted to be sent or received from a host or area that has been denied access.

Dual filters apply to a source and destination pair that allow traffic to flow or not flow between two specific hosts, areas, or combinations.

To specify the entity to be filtered, an address and mask must be used. Both are in the DECnet address format. Wherever the filter mask contains a zero, the corresponding address bit is ignored.

List of DECnet Packet Filters

Filter ID: This parameter is a decimal number that is selected according to the sequence in which you want the incoming traffic to be filtered. A filter with a lower ID number is affected before a filter with a higher ID number.

For example, when you want to permit a specific host access, but you want to deny access to the rest of the nodes in that area, the permit filter (specific host) must have a lower ID number than the deny (area) filter number. Otherwise, the deny filter would remove all traffic from that area, including the node on which you want to allow.

Required: Yes

Dependencies: This parameter is required to define DECnet filters.

Valid Values: 1 to 100

Default Value: None

Filter Type: This parameter specifies the type of filter for a specific ID. A singular filter identifies a node, an area, a subset of nodes belonging to an area, a subset of areas, or all nodes with a single expression. A dual filter identifies two end points from which to deny or allow traffic. The end points are each identified in the same way as a singular filter.

Required: No

Dependencies: This parameter is required when "Filter ID" is configured.

Valid Values: Singular, Dual

Default Value: Singular

Permit or Deny Traffic: This parameter specifies whether the traffic for a specific ID is permitted through the IBM 6611 or discarded.

Required: No

Dependencies: This parameter is required when "Filter ID" is configured.

Valid Values: Deny, Permit

Default Value: Permit

Filter DECnet Address 1: This parameter specifies the address of the node for a specific ID. For dual filters, this is one of the end points. For singular filters, this is the only end point.

Required: Yes

Dependencies: This parameter is required when "Filter ID" is configured.

Valid Values: 1.1 to 63.1023

Default Value: None

Filter Mask 1: This parameter specifies the mask for a specific DECnet ID. The mask in conjunction with “Filter DECnet Address 1” on page 3-120 dictates the range of addresses that can be filtered. Wherever the filter mask contains a zero, the corresponding address bit is insignificant. Therefore, if the mask is set to **0.0**, all of the address bits are ignored and all traffic is implied.

Required: No

Dependencies: This parameter is enabled when “Filter ID” is configured.

Valid Values: 0.0 to 63.1023

Default Value: 63.1023

Filter DECnet Address 2: This parameter specifies the address of the node for a specific filter ID. This parameter is for dual filters only and specifies the second of the two end points.

Required: No

Dependencies: This parameter is configured when “Filter Type” on page 3-120 is set to **Dual**.

Valid Values: 1.1 to 63.1023

Default Value: None

Filter Mask 2: This parameter specifies the mask for a specific ID. The mask in conjunction with the DECnet address dictates the range of addresses that are filtered. This parameter is for dual filters only. Wherever the filter mask contains a zero, the corresponding address bit is insignificant. Therefore, if the mask is set to **0.0**, the entire address is insignificant.

Required: No

Dependencies: This parameter is enabled when “Filter Type” on page 3-120 is set to **Dual**.

Valid Values: 0.0 to 63.1023

Default Value: 63.1023

Chapter 4. System Management Parameters

About this Chapter	4-2
IBM 6611 Names	4-3
EIA 232 Serial Ports	4-4
Lock or Unlock the Multiprotocol Network Program	4-5
Simple Network Management Protocol	4-6
Rules for Object Identifiers and Names	4-6
Enabling SNMP	4-6
SNMP System Parameters	4-7
Defining SNMP Traps	4-9
List of Clients Who Can Receive Traps	4-9
Defining Views	4-12
List of SNMP Views	4-12
List of SNMP MIB Subtrees	4-13
Defining Communities	4-13
List of SNMP Communities	4-14
Userids and Passwords	4-16
List of Controlling Users	4-16
List of Viewing Users	4-16
Configuration Hosts	4-18
List of Configuration Hosts for this IBM 6611	4-18
Time to Perform Configuration	4-19
Remote Host Names	4-21
List of Remote Host Names to IP Addresses	4-21
Name Servers	4-22
Time Servers	4-23

About this Chapter

This chapter provides information about the System Management parameters. System Management configures the parameters that are not adapter and protocol dependent. This chapter is designed as a reference for Chapter 1 and Appendix A.

Each parameter contains the following information:

Parameter Name	Provides the name of the parameter.
Description	Provides the function of the parameter.
Required	Tells you whether the parameter must be configured to complete the configuration.
Dependencies	Tells you about any related parameters that can affect the way this parameter is configured.
Valid Values	Provides the range of values that can be used.
Default Value	Provides the preset value in the Configuration Program.

IBM 6611 Names

Use the worksheet on page A-18.

IBM 6611 Host Name: This parameter defines the host name by which the IBM 6611 is identified to the network. When this name is configured with one of this IBM 6611's IP addresses by a remote IP node, it can also be used as a replacement for that IP address when accessing this IBM 6611 remotely over the IP network.

Required: No

Dependencies: This parameter is configured once for each IBM 6611.

Valid Values: A string of up to 31 alphanumeric characters. These characters can be separated by periods, underscores, or dashes.

Default Value: 6611host

Domain Name: The domain name is used to qualify hosts identified using the domain name server.

Required: No

Dependencies: This parameter is configured only when a domain name server is used in the network to qualify host names.

Valid Values: A string of up to 63 alphanumeric characters. These characters can be separated by periods.

Default Value: None

EIA 232 Serial Ports

Use the worksheet on page A-18.

The parameters in this section are used to configure the EIA 232 serial ports S1 and S2 (labelled S1 and S2 on the Model 120 and Model 170, and labelled Serial 1 and Serial 2 on the Model 140). The serial ports are used to service the IBM 6611. They can be set up for local use when attaching an ASCII terminal. They can be configured for remote use by attaching a modem that is connected to the public switched network.

Baud Rate for S1 Serial Port: This parameter defines the speed at which the data is transmitted to and from a device. For a direct-attached terminal, 9600 bps normally should be configured. For a modem-attached terminal, 1200 or 2400 bps should be configured.

Required: No

Dependencies: None

Valid Values: 1200 bps, 2400 bps, 9600 bps, 19200 bps, 38400 bps

Default Value: 9600 bps

Baud Rate for S2 Serial Port: This parameter defines the speed at which the data is transmitted to and from a device. For a direct-attached terminal, 9600 bps normally should be configured. For a modem-attached terminal, 2400 bps should be configured.

Required: No

Dependencies: When "Cylink Serial Number" on page 5-10 is configured, this parameter must match the baud rate configured on the Cylink 4201 for its EIA 232 port.

Valid Values: 1200 bps, 2400 bps, 9600 bps, 19200 bps, 38400 bps

Default Value: 2400 bps

Lock or Unlock the Multiprotocol Network Program

The purpose of this parameter is to be able to lock or unlock the Multiprotocol Network Program when it is being sold to a third-party customer. The software is locked by the original owner and unlocked by the customer to whom it is being sold.

This configuration parameter is activated on the IBM 6611 using a startup diskette. When the startup diskette is created by the Configuration Program, the diskette is placed in the diskette drive on a powered-off IBM 6611. The IBM 6611 is then powered on. The IBM 6611 locks or unlocks the Multiprotocol Network Program when it reads the diskette. The Multiprotocol Network Program on the IBM 6611 runs only when this parameter is set to **Unlock** on the startup diskette.

Lock Value: This parameter locks or unlocks the software on the IBM 6611. When the IBM 6611 is unlocked and is restarted using the configuration diskette with this parameter set to **Lock**, the software is disabled. When the IBM 6611 is in a locked state and is restarted using the configuration diskette with this parameter set to **Unlock**, the software unlocks. This parameter does not affect configuration when it is set to **Unlock** and the Multiprotocol Network Program is unlocked already.

Required: No

Dependencies: None

Valid Values: Lock, Unlock

Default Value: Unlock

Simple Network Management Protocol

Use the worksheet on page A-18.

The Simple Network Management Protocol (SNMP) is part of the TCP/IP suite of protocols. It is used to manage devices in an IP-based internet. SNMP works in the network by having the devices to be managed, such as IBM 6611s or specific hosts, running a program called the *SNMP agent*. At least one host in the internet must be running a program called the *SNMP client*. The hosts that run the SNMP clients are usually workstations operated by network operations personnel and are often referred to as *network management stations*. The SNMP client program usually is referred to as a *network management and network monitoring application*. In the case of TCP/IP, all management and monitoring is provided through SNMP clients and SNMP agents. This is achieved by the following interactions that the two types of programs support. SNMP clients support queries to SNMP agents in the IP network. After a query is sent by the SNMP client, the SNMP agent receives the message over the internet and responds to the query when the host computer sending the query is authorized to make such a request. If the client is authorized, the SNMP agent looks at the information that it maintains in its database, called a Management Information Base (MIB), and returns the result. Although SNMP architecture defines the ability of a client to set the values of variables in an SNMP agent's MIB, the IBM 6611 does not support *sets*. Another interaction that occurs between SNMP agents and clients is problem reporting. In these situations, the SNMP agent discovers a problem in the device it is monitoring. When a problem is discovered, the agent software creates a *trap* message and sends it over the IP internet to one or more SNMP clients that the agent had been configured to notify.

Restrictions: SNMP can be transported only over links that are configured for IP. The network administrator ensures that the IBM 6611 configured is reachable via IP.

Rules for Object Identifiers and Names

Some parameters require the specification of object identifiers or object names. The following rules apply:

1. An object identifier is specified in dotted numeric notation and must consist of three elements. The maximum number of elements in the object identifier is 50. Elements are separated by a decimal point. The first element must be a single digit in the range of 0 to 2. The second element must be an integer in the range of 1 to 40. The third and subsequent elements must be integers in the range of 1 to the size of an unsigned integer.
2. An object name consists of a textual name with an optional numeric instance that does not exceed a total of 128 characters. The object name must be known to the SNMP agent. Object names typically are names of nodes in the MIB tree. When the root of the MIB tree, *iso*, is specified as an object name, the numeric instance is required. A decimal point separates the textual name from the numeric instance.

Enabling SNMP

It is recommended that SNMP be enabled to facilitate management of the router from an external location. Completion of the SNMP configuration parameters will allow the router to accept SNMP requests and send SNMP traps to network management clients. SNMP configuration parameters also provide information used in MIB variables to identify the router.

Enable SNMP: This parameter enables and disables SNMP configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

SNMP System Parameters

This group of parameters provides the following:

- Identify the name, contact, location, and serial number of the IBM 6611. This information provides values for MIB variables that can be queried from an SNMP client.
- Control the filtering of identical enterprise-specific traps.

System Contact: This parameter provides the name and phone number of the contact person who is responsible for the IBM 6611. The value for system contact is maintained in the MIB variable *sysContact*.

Required: Yes

Dependencies: This parameter is required when “Enable SNMP” on page 4-6 is set to **Enable**.

Valid Values: A string of 1 to 255 ASCII characters.

Default Value: None

System Name: This parameter provides the administratively assigned name of the node. By convention, this is the node’s fully qualified domain name. The value specified for system name is maintained in the MIB variable *sysName*.

Required: Yes

Dependencies: This parameter is required when “Enable SNMP” on page 4-6 is set to **Enable**.

Valid Values: A string of 1 to 255 ASCII characters

Default Value: None

System Location: This parameter provides directions to the geographic location of the IBM 6611 (for example, telephone closet, 3rd floor, 812 Whyte Avenue). The value specified for system location is maintained in the MIB variable *sysLocation*.

Required: Yes

Dependencies: This parameter is required when “Enable SNMP” on page 4-6 is set to **Enable**.

Valid Values: A string of 1 to 255 ASCII printable characters. New lines and blanks may be included.

Default Value: None

Enterprise-Specific Trap Throttle Time: This parameter defines the number of seconds that must separate consecutive enterprise-specific traps with an identical ID or number in order for them to be sent to clients as separate traps. A value of zero indicates that all traps are to be sent.

The IBM 6611 contains a mechanism to prevent sending consecutive enterprise-specific traps with identical IDs or numbers. This prevents unnecessary network traffic and unnecessary network operator interruptions. The following logic is implemented in the IBM 6611:

- The value specified in this parameter is maintained in the *ibmTrapThrottleID* MIB variable.
- The ID/number of the last enterprise-specific trap sent is maintained in the *ibmTrapThrottleID* MIB variable.
- When a trap condition occurs, the IBM 6611 checks to see if it has the same specific trap ID/number as *ibmTrapThrottleID* (the last trap sent).
 - If the ID or number is identical and the current time minus the time of the last trap is less than the value specified in *ibmTrapThrottleTime*, the value of *ibmTrapThrottleCount* is incremented and the trap is not sent.
 - If the ID or number is not identical, or it is identical and the current time minus the time of the last trap is greater than or equal to the value specified in *ibmTrapThrottleTime*, the trap is sent.
 - If *ibmTrapThrottleCount* is not 0, the *ibmTrapThrottleCount* and *ibmTrapThrottleID* MIB variables are included in the trap.
 - *ibmTrapThrottleCount* is set to 0.

Required: No

Dependencies: This parameter affects only those clients configured to receive enterprise-specific traps. “Enable enterpriseSpecific Trap” on page 4-12 specifies that enterprise-specific traps are to be sent when the parameter is set to **Enable**.

Valid Values: 0 to 3600 seconds

Default Value: 900 seconds

Router Serial Number Prefix: This parameter defines the serial number of the router, which is located on the :

- Front panel to the right of the 3-digit display of the Model 120
- Front panel below the 3-digit display of the Model 140
- Top cover of the Model 170.

It is also located on a bar-code label on the back of the IBM 6611s. The serial number can be up to 10 characters long (composed of a 2-character plant-of-manufacture code, a dash, and a 7-character sequence number). This parameter is the plant-of-manufacture part of the serial number.

The router serial number provides a portion of the MIB variable *sysDescr*. The plant-of-manufacture, the characters before the dash, are maintained in the MIB variable *plantOfManufacture*. The sequence number, the characters after the dash, are maintained in the MIB variable *seqNum*.

Required: Yes

Dependencies: This parameter is required only if “Enable SNMP” on page 4-6 is set to **Enable**. The values of this parameter and the “Router Serial Number Suffix” make up the entire serial number. This serial number is an additive string composed of the values of each parameter separated by a dash.

Valid Values: A string containing 2 alphanumeric characters. All alphabetic characters must be in upper case.

Default Value: None

Router Serial Number Suffix: This parameter defines the serial number of the router, which is located on the:

- Front panel to the right of the 3-digit display of the Model 120
- Front panel below the 3-digit display of the Model 140
- Top cover of the Model 170.

It is also located on a bar-code label on the back of the IBM 6611s. The serial number can be up to 10 characters long (composed of a 2-character plant-of-manufacture code, a dash, and a 7-character sequence number). This parameter is the sequence number part of the serial number.

The router serial number provides a portion of the MIB variable *sysDescr*. The plant-of-manufacture, the characters before the dash, are maintained in the MIB variable *plantOfManufacture*. The sequence number, the characters after the dash, are maintained in the MIB variable *seqNum*.

Required: Yes

Dependencies: This parameter is required only if “Enable SNMP” on page 4-6 is set to **Enable**. The values of this parameter and the “Router Serial Number Prefix” make up the entire serial number. This serial number is an additive string composed of the values of each parameter separated by a dash.

Valid Values: A string containing up to 7 alphanumeric characters

Default Value: None

Defining SNMP Traps

The following parameters provide specifications for each SNMP client to which the router should send SNMP traps. At least one SNMP client must be configured. However, there is no limit on how many can be defined.

List of Clients Who Can Receive Traps

The parameters in the following list are configured for each SNMP client to which the router sends SNMP traps:

- “Trap Address (IP Address or Domain Name)” on page 4-10
- “Trap Community Name” on page 4-10
- “Enable coldStart Trap” on page 4-10
- “Enable warmStart Trap” on page 4-10
- “Enable linkDown Trap” on page 4-11
- “Enable linkUp Trap” on page 4-11
- “Enable authenticationFailure Trap” on page 4-11
- “Enable egpNeighborLoss Trap” on page 4-12
- “Enable enterpriseSpecific Trap” on page 4-12.

Trap Address (IP Address or Domain Name): Traps generated by the IBM 6611 are sent to the host in the SNMP client specified by this parameter. The trap address is an IP address or host name.

Note: Assume that the specified host is receiving on UDP port 162 for SNMP traps.

Required: Yes

Dependencies: This parameter is required when “Enable SNMP” on page 4-6 is set to **Enable**.

This parameter is configured for each SNMP client to which the router sends SNMP traps.

Valid Values: An IP address or Domain Name

Default Value: None

Trap Community Name: This parameter defines the community name encoded in the trap packet that is sent to a particular client.

Required: No

Dependencies: This parameter is configured for each SNMP client to which the router sends SNMP traps.

If the default is used, the IBM 6611 can send traps to all clients that allow public access.

Valid Values: An alphanumeric string 1 to 63 characters long

Default Value: Public

Enable coldStart Trap: This parameter determines whether the SNMP *coldStart*. A *coldStart* trap signifies that the IBM 6611 is reinitializing itself such that the SNMP agent's configuration or the SNMP implementation is altered.

Required: No

Dependencies: This parameter is configured for each SNMP client to which the router sends SNMP traps.

Valid Values: Enable, Disable

Default Value: Enable

Enable warmStart Trap: This parameter determines if the SNMP *warmStart* trap is sent to the IP address configured in “Trap Address (IP Address or Domain Name).”

A *warmStart* trap signifies that the IBM 6611 is reinitializing itself. Therefore, the SNMP agent configuration or the SNMP implementation is not altered.

Required: No

Dependencies: This parameter is configured for each SNMP client to which the router sends SNMP traps.

Valid Values: Enable, Disable

Default Value: Enable

Enable linkDown Trap: This parameter determines whether the SNMP *linkDown* trap is sent to the IP address in the “Trap Address (IP Address or Domain Name)” on page 4-10.

A *linkDown* trap signifies that the IBM 6611 detects that one of its communication ports is not operational. The trap contains the *ifIndex* MIB variable to identify the affected port.

Required: No

Dependencies: This parameter is configured for each SNMP client to which the router sends SNMP traps.

Valid Values: Enable, Disable

Default Value: Enable

Enable linkUp Trap: This parameter determines if the SNMP *linkUp* trap is sent to the IP address configured in “Trap Address (IP Address or Domain Name)” on page 4-10.

A *linkUp* trap signifies that the IBM 6611 detects that one of its communication ports is operational. The trap contains the *ifIndex* MIB variable to identify the port that is affected.

Required: No

Dependencies: This parameter is configured for each SNMP client to which the router sends SNMP traps.

Valid Values: Enable, Disable

Default Value: Enable

Enable authenticationFailure Trap: This parameter determines whether the SNMP *authenticationFailure* trap is sent to the IP address configured in “Trap Address (IP Address or Domain Name)” on page 4-10.

An *authenticationFailure* trap signifies that the IBM 6611 received an SNMP request that is not correctly authenticated. This means that the community IP address or domain name and community name do not map to an authorized community as configured in “Community Name” on page 4-14 and “Community Address (IP Address or Domain Name)” on page 4-14.

Required: No

Dependencies: This parameter is configured for each SNMP client to which the router sends SNMP traps.

Valid Values: Enable, Disable

Default Value: Enable

Enable *egpNeighborLoss* Trap: This parameter determines whether the SNMP *egpNeighborLoss* trap is sent to the IP address configured in “Trap Address (IP Address or Domain Name)” on page 4-10.

An *egpNeighborLoss* trap signifies that an EGP neighbor for whom the IBM 6611 was an EGP peer has been marked down and that the peer relationship no longer exists. The trap contains an instance of the *egpNeighAddr* MIB variable that identifies the affected neighbor.

Required: No

Dependencies: This parameter is configured for each SNMP client to which the router sends SNMP traps.

Valid Values: Enable, Disable

Default Value: Enable

Enable *enterpriseSpecific* Trap: This parameter determines whether the SNMP *enterpriseSpecific* trap is sent to the IP address configured in “Trap Address (IP Address or Domain Name)” on page 4-10.

An *enterpriseSpecific* trap signifies that the IBM 6611 detects an event that occurred. The event is unique to the IBM 6611, a specific protocol, or transmission media. The *enterpriseSpecific* trap parameter uniquely identifies the particular trap that occurred. IBM 6611-specific traps contain MIB variables to identify problem description, probable causes, recommended actions, and failure-specific data.

Required: No

Dependencies: This parameter is configured for each SNMP client to which the router sends SNMP traps.

Valid Values: Enable, Disable

Default Value: Enable

Defining Views

List of SNMP Views

View Name: This parameter names the view in dotted numeric notation that is configured in “MIB Subtree” on page 4-13.

Required: No

Dependencies: This parameter is required to define SNMP views. This parameter must match the value configured in “Community View Name” on page 4-15.

Valid Values: See “Rules for Object Identifiers and Names” on page 4-6.

Default Value: None

List of SNMP MIB Subtrees

MIB Subtree: This parameter provides a list of MIB groups (subtrees) configured as an object name or an object identifier in “View Name” on page 4-12. All objects derived from other objects are defined by the subtree names and are placed in the view.

Required: No

Dependencies: This parameter is required to define SNMP MIB subtrees. This parameter and “View Name” must be configured for each view the router supports.

Valid Values: See “Rules for Object Identifiers and Names” on page 4-6.

Default Value: None

Defining Communities

The SNMP agent in the router uses a simple authentication scheme to determine which network management stations (SNMP clients) can access its MIB variables. This authentication scheme involves the specification of SNMP access policies. An SNMP access policy is an administrative relationship involving an association among an SNMP community, an access mode, and a MIB view.

An SNMP community is defined by a group of one or more SNMP clients and a community name. A community name is a string of octets that an SNMP client must imbed in an SNMP request packet for authentication purposes.

The access mode specifies the access the SNMP clients in the community are allowed in order to retrieve and modify the MIB variables managed by the SNMP agent in the IBM 6611. The access mode must be *None* or *ReadOnly*.

A MIB view defines one or more MIB subtrees that a specific SNMP community can access. The MIB view can be the entire MIB tree or a limited subset of the entire MIB tree.

When the SNMP agent in the IBM 6611 receives a request, it verifies the community name with the requesting IP address of the SNMP client to determine when the requesting client is a member of the SNMP community identified by the community name. When the requesting client is a member of the SNMP community, then the SNMP agent determines when the requesting client is allowed the specified access for the specified MIB variables as defined in the access policy associated with that community. If all the criteria are met, the SNMP agent attempts to honor the request. Otherwise, the SNMP agent generates an *authenticationFailure* trap or returns the appropriate error message to the requesting client.

At least one SNMP Community must be configured. There is no limit to the number of SNMP communities allowed. By default, a community name of “public,” a community IP address or domain name of “0.0.0.0” and a community address mask of “0.0.0.0” are provided. This allows any host to query this router using a community name of “public.” When this configuration does not meet your requirements, you should delete or modify the existing community and add additional communities using the following parameters. Refer to *IBM 6611 Network Processor Network Management Reference*.

List of SNMP Communities

Community Name: This parameter provides a community name that must be used by an SNMP client to access the MIB in the IBM 6611.

An SNMP community consists of one or more SNMP clients and a community name. The data provided by this parameter and "Community Address (IP Address or Domain Name)" defines the SNMP community.

If the entry includes no periods, it is considered a Domain Name.

If it contains a period and the first character is numeric, it is validated as an IP Address.

If it contains a period and the first character is alphabetic, it is validated as a Domain Name.

A Domain Name can contain only alphanumeric characters and a period. No imbedded blanks are allowed.

Required: Yes

Dependencies: This parameter is required only if "Enable SNMP" on page 4-6 is set to **Enable** and a community is being defined.

Valid Values: A string of 1 to 63 alphanumeric characters

Default Value: None

Community Address (IP Address or Domain Name): This parameter defines the address of the host in this community from which the IBM 6611 should accept requests. If the address is specified as "0.0.0.0", the router will accept SNMP requests from any host address as long as the request contains the name of this community. The address is either an IP address or a host name. A host name is allowed only when a name server is available to the IBM 6611 in the network.

An SNMP community is defined by one or more SNMP clients and a community name. The data provided by "Community Name" and this parameter defines the SNMP community.

Required: No

Dependencies: None

Valid Values: 0.0.0.0 to 255.255.255.255, or a valid domain name

Default Value: 0.0.0.0

Community Address Mask: This parameter is a network mask in dotted decimal format for the specified "Community Address (IP Address or Domain Name)."

Required: No

Dependencies: None

Valid Values: 0.0.0.0 to 255.255.255.255

Default Value: 255.255.255.255

Community Access: This parameter determines the access granted to the community when accessing the MIB in the IBM 6611.

Required: No

Dependencies: None

Valid Values: Read only, None

Default Value: Read only

Community View Name: This parameter determines the view used by this community when accessing the MIB. The view is configured in "View Name" and "MIB Subtree." This view determines the MIB objects that this community can access. When a view name is not specified, the view defaults to all objects defined to the router's SNMP agent are used.

Required: No

Dependencies: This parameter must match a value configured in "View Name."

Valid Values: See "Rules for Object Identifiers and Names" on page 4-6.

Default Value: None

Userids and Passwords

Use the worksheet on page A-19.

There are two classes of users: controlling and viewing. There can be multiple controlling and viewing users. There are two default userids preconfigured on the IBM 6611. One is a controlling userid and the other is a viewing userid. The controlling userid and password is `ibm6611c`. The viewing userid and password is `ibm6611v`.

Note: IBM recommends that you delete these userids or change the passwords immediately after receiving the IBM 6611.

A maximum of 10 system users can be logged into the IBM 6611 at one time. A controlling userid can be changed and other controlling and viewing userids can be added using the System Manager or subsequent configuration of the following parameters. For more information, see "Logging In to an IBM 6611" on page 9-23.

List of Controlling Users

Controlling Userid: This parameter defines the login for a controlling user to access the IBM 6611.

Required: No

Dependencies: This parameter must be configured with the "Controlling Password."

Valid Values: A string of up to 8 alphanumeric lowercase characters. The string must start with an alphabetic character.

Default Value: None

Controlling Password: This parameter sets the password associated with the controlling userid in "Controlling Userid."

Required: No

Dependencies: This parameter must be configured with "Controlling Userid."

Valid Values: A string of up to 8 alphanumeric lowercase characters. The string must start with an alphabetic character.

Default Value: None

List of Viewing Users

Viewing Userid: This parameter defines the login userid for a viewing user to access the IBM 6611.

Required: No

Dependencies: This parameter must be configured with "Viewing Password" on page 4-17.

Valid Values: A string of up to 8 alphanumeric lowercase characters. The string must start with an alphabetic character.

Default Value: None

Viewing Password: This parameter defines the password associated with the viewing user login userid in "Viewing Userid."

Required: No

Dependencies: This parameter must be configured with "Viewing Userid" on page 4-16.

Valid Values: A string of up to 8 alphanumeric lowercase characters. The string must start with an alphabetic character.

Default Value: None

Configuration Hosts

The following parameters configure the IP addresses of remote hosts in the IP network that can perform remote configuration to this IBM 6611. By default, all hosts can perform configuration. There is no limit to the number of hosts that can be configured.

Hosts that can perform configuration functions on this IBM 6611: If **All hosts** is selected, configuration parameters can be sent to the IBM 6611 by any host in the IP network.

If **List of specific hosts** is selected, the IP address and address mask must be configured for each host that is allowed to connect directly from the Configuration Program to the IBM 6611 and perform configuration functions. This function does not prevent the configuration that is performed from the Configuration Program using a diskette, nor does it prevent the configuration that is performed using the System Manager.

Required: No

Dependencies: None

Valid Values: All hosts, List of specific hosts

Default Value: All hosts

List of Configuration Hosts for this IBM 6611

IP Address: This parameter defines the IP address of a remote host that is allowed to connect directly from the Configuration Program to the IBM 6611 and perform configuration functions. This parameter has no effect on the configuration that is performed from the Configuration Program using a diskette or the configuration that is performed using the System Manager.

Required: No

Dependencies: This parameter is required when "Hosts that can perform configuration functions on this IBM 6611" is set to **List of specific hosts**.

Valid Values: A valid IP address

Default Value: None

Address Mask: This parameter defines a number of remote hosts by combining the mask with the IP address that is defined in "IP Address." Each bit in the mask that is a zero causes the same relative bit in the address to be ignored. This can be used to allow all hosts on one particular network or subnetwork to perform remote configuration on this IBM 6611.

Required: No

Dependencies: This parameter is required when "Hosts that can perform configuration functions on this IBM 6611" is set to **List of specific hosts**.

Valid Values: A 4-octet dotted number where each octet is between 0 to 255.

Default Value: 255.255.255.255

Time to Perform Configuration

This function allows you to build a configuration and to specify when it should be applied by the IBM 6611. This function is designed to be used with configurations built by the Configuration Program using either a direct connection or a diskette. If you specify a time delay for the configuration (Apply Configuration not defaulted to **Immediately**) and this configuration is built from the System Manager, the configuration should be committed immediately. You cannot reject a time-delayed configuration.

Apply Configuration: This parameter defines when to apply the configuration to the IBM 6611.

Required: No

Dependencies: If **At a specific time and day** is selected, "Year," "Month," "Day," "Hour," and "Minute" parameters must be configured.

Valid Values: Immediately, At next IML, At a specific time and day

Note: The configuration file on the diskette that is installed in the diskette drive will be read only when a power-on reset (POR) initiated. Any configuration that is loaded into the 6611 via any other method will be loaded based on the value specified (Immediately, next IML, Date Time).

Default Value: Immediately

Year: This parameter defines the year in which the configuration is to be applied.

Note: This parameter assumes that the date on the IBM 6611 is correct.

Required: No

Dependencies: The "Apply Configuration" parameter must be set to **At a specific time and day**.

Valid Values: 1991 to 9999

Default Value: Current Year

Month: This parameter defines the month when the configuration is to be applied.

Note: This parameter assumes that the date on the IBM 6611 is correct.

Required: No

Dependencies: The "Apply Configuration" be set to **At a specific time and day**.

Valid Values: 1 to 12

Default Value: Current month

Day: This parameter defines the day when the configuration is to be applied.

Required: No

Dependencies: The “Apply Configuration” must be set to **At a specific time and day**.

Note: This parameter assumes that the date on the IBM 6611 is correct.

Valid Values: 1 to 31

Default Value: Current day

Hour: This parameter defines the hour when the configuration is to be applied.

Required: No

Dependencies: The “Apply Configuration” on page 4-19 must be set to **At a specific time and day**.

Note: This parameter assumes that the time on the IBM 6611 is correct.

Valid Values: 0 to 23 (0 to 11 is AM, 12 to 23 is PM)

Default Value: Current hour

Minute: This parameter defines the minute when the configuration is to be applied.

Note: This parameter assumes that the time on the IBM 6611 is correct.

Required: No

Dependencies: The “Apply Configuration” on page 4-19 must be set to **At a specific time and day**.

Valid Values: 0 to 59

Default Value: Current minute

Remote Host Names

Use the worksheet on page A-19.

The list of remote host names and addresses defines a list of host names matched with IP addresses to access remote IP nodes. These parameters are not required. You can define as many hosts as you want. The purpose of defining host names is to allow you to use a host name instead of an IP address when referring to a host node for remote access. Correlating the host name to an IP address using these parameters works only for the IBM 6611 that is being configured. For consistency, this mapping must be done throughout the IP network for each device and host.

List of Remote Host Names to IP Addresses

IP Address of Host: This parameter defines the IP address of the host that has the symbolic name given in "Host Name."

Required: No

Dependencies: This parameter must be configured with "Host Name."

Valid Values: A valid IP address

Default Value: None

Host Name: This parameter is the symbolic name that is mapped to the IP address in "IP Address of Host."

Required: No

Dependencies: This parameter must be configured with "IP Address of Host."

Valid Values: A string of up to 31 alphanumeric characters

Default Value: None

Name Servers

These parameters enable the forwarding of name service requests to one or more remote name servers provided in a list of name servers. See “IP Address of Name Server.” These parameters are not required.

Enable Name Resolution by Remote Name Servers: This parameter enables or disables name resolution using one or more remote name servers running in the IP network. When enabled, this IBM 6611 resolves symbolic names by sending a name service request to one or more of the name servers in a list of IP addresses.

Required: No

Dependencies: This parameter is configured once for each remote name server.

Valid Values: Enable, Disable

Default Value: Disable

IP Address of Name Server: This parameter defines the IP address of a name server that is operating in the network.

Required: Yes

Dependencies: This parameter is required when “Enable Time Service by Remote Time Servers” is set to **Enable**.

Valid Values: A valid IP address

Default Value: None

Time Servers

Enable Time Service by Remote Time Servers: This parameter enables or disables remote time service. Remote time service allows the IBM 6611 to get its time from another IP node that has a time server application installed on the network. When enabled, this IBM 6611 gets its time from a remote time server in the list of remote time servers by sending a time service request. When the first remote time server listed is unable to provide time service, the request is sent to the second remote time server.

Required: No

Dependencies: This parameter is configured one for each remote time server.

Valid Values: Enable, Disable

Default Value: Disable

IP Address of Remote Time Server: This parameter defines the IP address of a remote time server that is operating in the IP network. This parameter is defined for each time server.

Required: No

Dependencies: This parameter is required when “Enable Time Service by Remote Time Servers” is set to **Enable**.

Valid Values: A valid IP address

Default Value: None

Chapter 5. Adapter Configuration Parameters

About this Chapter	5-2
Token-Ring Network 16/4 Adapter	5-3
Physical Interface	5-3
Ethernet Adapter	5-6
List of Multicast MAC Addresses	5-8
EIA 422/449 Serial Adapter and V.35/V.36 Serial Adapter	5-9
Physical Interface	5-10
LAN Bridging Protocol	5-12
Network Management Parameters	5-14
Passwords to Link Network Managers	5-14
Point-to-Point Protocol (PPP)	5-16
Frame Relay	5-18
List of DLCI Numbers	5-20
SDLC Adapter	5-21
Physical Interface	5-22
SDLC Adapter SNA Stations	5-25
List of SNA Stations	5-25
SNA Station Detail	5-27
X.25 Adapter	5-30
SVC Packet Sizes	5-30
SVC Packet Window Sizes	5-31
Subscription Mapping	5-33
Logical Channel Parameters	5-33
Subscription Mapping 2	5-35
Auto-Call Options	5-36
PVC Settings	5-37
List of PVCs	5-37
PVC Default Settings	5-38
SVC Defaults	5-39
Facilities Control	5-41
Closed User Group (CUG) Selection Facility	5-43
X.25 Network Tuning	5-44
IP	5-45
Frame Level Tuning	5-45
Packet Level Tuning	5-45
Physical Level Tuning	5-46
IP/X.25 Mapping	5-47
List of X.25 Remote Hosts	5-47
Optional SVC Parameters	5-48

About this Chapter

This chapter provides information about the various adapter parameters. This chapter is designed as a reference for Chapter 1 and Appendix A.

Each parameter contains the following information:

Parameter Name	Provides the name of the parameter.
Description	Provides the function of the parameter.
Required	Tells you whether the parameter must be configured to complete the configuration.
Dependencies	Tells you about any related parameters that can affect the way this parameter is configured.
Valid Values	Provides the range of values that can be used.
Default Value	Provides the preset value in the Configuration Program.

See “Configuration Considerations” on page 1-10 for information about changing configuration parameters.

Token-Ring Network 16/4 Adapter

Use the worksheet on page A-20.

The Token-Ring Network 16/4 Adapter enables an IBM 6611 to attach to an IEEE 802.5 network, such as the IBM Token-Ring Network. "Token-Ring Data Rate" on page 5-5 must be configured to match the data rate of the token ring to which it is attached. The choices are 4 Mbps or 16 Mbps.

After you configure the Token-Ring Network 16/4 Adapter parameters, configure the protocols for which you want the adapter to transmit and receive frames.

Restrictions: None

Compatible Protocols: The Token-Ring Network 16/4 Adapter supports the following protocols:

- For routing:
 - IP
 - IPX
 - XNS
 - DECnet
 - AppleTalk
- For bridging, any protocols including the following:
 - IP
 - IPX
 - XNS
 - DECnet
 - SNA
 - NetBIOS
 - AppleTalk
- For data link switching:
 - NetBIOS
 - APPN
 - SNA.

Physical Interface

Enable Interface: This parameter enables or disables the Token-Ring Network 16/4 Adapter port. The adapter has one port. Select **Enable** when you want the port to be active on the token-ring network.

When the port is enabled, the Multiprotocol Network Program uses the values of the other Token-Ring Network 16/4 Adapter parameters to initialize the port. When the port is disabled, the values are not used but are retained in the configuration file.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

MAC Address: This parameter indicates whether you want to use the adapter medium access control (MAC) address or the locally administered address as the adapter's MAC layer address. The MAC sublayer address is the physical address that the adapter uses to receive and transmit frames.

The Token-Ring Network 16/4 Adapter has a unique, adapter MAC address that the manufacturer encoded in the adapter's ROM. The adapter MAC address is 12 hexadecimal digits long.

The locally administered address is a MAC layer address that you determine. The locally administered address is 12 hexadecimal digits long and overrides the universally administered address. The address should be typed using the format configured in "MAC Address Format."

Ensure that the locally administered MAC address ("Locally Administered Address") is unique on your network and is not a reserved value; for example: X'1111 1111 1111' is the broadcast address.

Select **Universally Administered Address** when you do not want to specify a locally administered address for the adapter.

Note: When you configure DECnet on this adapter, it overrides the universally administered address automatically with the DECnet locally administered address that is derived from the value you select for "Local DECnet Address" on page 3-116.

Required: No

Dependencies: When you do not select **Universally administered address**, you must specify a locally administered MAC address that you want to use as the adapter's MAC layer address.

Valid Values: Universally administered address, Locally administered address

Default Value: Universally administered address

Locally Administered Address: This parameter defines the locally administered address. If you select **canonical**, the range is as follows:

X'x2xx xxxx xxxx'
X'x6xx xxxx xxxx'
X'xAxx xxxx xxxx'
X'xExx xxxx xxxx'.

where x is any value X'0' to X'F'.

If you select **non-canonical**, the valid values are as follows:

X'4000 0000 0000' to X'7FFF FFFF FFFF'

Required: Yes

Dependencies: This parameter is required when "MAC Address" on page 5-3 is set to **Locally Administered Address**.

Valid Values: X'4000 0000 0000' to X'7FFF FFFF FFFF'

Default Value: None

MAC Address Format: This parameter determines which format is used for the locally administered address.

The non-canonical format is more common for token-ring users. The bit ordering is exactly the same as the sequence that goes out on the wire, which requires the most significant bit of each byte to be transmitted first.

The canonical format is defined by the IEEE 802.2 standard. Non-canonical MAC addresses can be converted to canonical by rotating each byte so that the least significant bit is switched to the most significant bit. The second least significant bit becomes the second most significant bit, and so on. Each byte remains in its original position.

Required: No

Dependencies: When “MAC Address” on page 5-3 is set to **Locally administered address**, this parameter must be configured.

Valid Values: Non-canonical, Canonical

Default Value: Non-canonical

Token-Ring Data Rate: This parameter defines the data transfer rate that you want the Token-Ring Network 16/4 Adapter to use.

Select the data rate that matches the data transfer rate for the ring to which the adapter is connected. If the ring is operating at 4 Mbps, you must select **4 Mbps**.

Warning: The adapter data rate must match the data rate of the ring to which it is attached. If it does not, the rings become inactive until this adapter is forced off the ring. To correct this problem, you must reconfigure the correct data rate for this adapter.

Required: No (Yes, when the physical interface is enabled)

Dependencies: None

Valid Values: 4 Mbps, 16 Mbps

Default Value: None

Broadcast Type: When this parameter is set to **Local**, it allows this IBM 6611 to communicate with stations on a local token ring. When this parameter is set to **Non-local**, it allows this IBM 6611 to communicate with stations on the local ring, and to stations that are connected to your ring through source route bridging.

Required: No

Dependencies: None

Valid Values: Non-local, Local

Default Value: Non-local

Ethernet Adapter

Use the worksheet on page A-20.

The Ethernet Adapter enables an IBM 6611 to attach to an IEEE 802.3 network or to an Ethernet Version 2 network. The adapter has one port, which you can configure to support IEEE 802.3, Ethernet Version 2, and IEEE Ethernet SNAP.

After you configure the Ethernet Adapter parameters, configure the protocols that you want the adapter to transmit and receive.

Restrictions: None

Compatible Protocols: The Ethernet Adapter supports the following protocols:

- For routing:
 - IP
 - IPX
 - XNS
 - DECnet
 - AppleTalk
- For bridging, any protocols including the following:
 - IP
 - IPX
 - XNS
 - DECnet
 - SNA
 - NetBIOS
 - AppleTalk
- For data link switching:
 - NetBIOS
 - APPN
 - SNA.

Enable Interface: This parameter enables or disables the Ethernet Adapter port. Select **Enable** when you want the port to be active on the network.

When the port is enabled, the Configuration Program uses the values of the other Ethernet Adapter parameters to initialize the port. When disabled, the port cannot transmit nor receive data.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

MAC Address: This parameter indicates whether you want to use the address that is encoded in the adapter's ROM. The MAC layer address is the physical address that the adapter uses to receive and transmit frames. The universally administered address is 12 hexadecimal digits. Select **Universally administered address** when you do not want to specify a locally administered address for the adapter.

The locally administered address is a MAC layer address that you assign when you do not use the universally administered address. The locally administered address is 12 hexadecimal digits and overrides the universally administered address.

Ensure that the locally administered address is unique on your network and is not a reserved value: for example, X'FFFF FFFF FFFF' is the broadcast address.

Required: No

Dependencies: When you do not select **Universally administered address**, you must specify "Locally Administered Ethernet MAC Address."

Note: When you configure DECnet for this adapter, it automatically overrides the universally administered address with the DECnet locally administered address, which is configured in "Local DECnet Address" on page 3-116.

Valid Values: Universally administered address, Locally administered address

Default Value: Universally administered address

Locally Administered Ethernet MAC Address: This parameter defines a 48-bit hardware address (locally administered address) defined by this parameter. The address should be entered in canonical format.

In a locally administered address, the multicast bit should be 0, and the local bit should be 1. Therefore, the first byte should be X'XXXX XX10'. A valid example of a locally administered address is X'0211 2233 4455'.

Required: Yes

Dependencies: This parameter is required when "MAC Address" on page 5-6 is set to **Locally Administered Address**.

Valid Values: If you select **canonical**, the range is as follows:

X'x2xx xxxx xxxx'
X'x6xx xxxx xxxx'
X'xAxx xxxx xxxx'
X'xExx xxxx xxxx'

where x is any value X'0' to X'F'.

Default Value: None

Enable Additional Multicast Addresses: This parameter allows the Ethernet Adapter to receive frames that are addressed to a group of adapters. The members of the group are identified by a common multicast address. The multicast address is used only in multicast frames. Non-multicast frames contain either the universally administered or the locally administered MAC layer address.

Required: No

Dependencies: When you set this parameter to **Allow**, you must configure at least one "Multicast MAC Address."

Note: Multicast addresses will be used by some protocols (such as OSPF) even if this parameter is configured as **Disable**.

Valid Values: Enable, Disable

Default Value: Disable

List of Multicast MAC Addresses

A maximum of 256 multicast MAC address can be configured.

Multicast MAC Address: The Ethernet Adapter receives frames that are addressed to the multicast MAC address that you specify in this entry field. This multicast address is a MAC layer address and must comply with the IEEE 802.3 or the Ethernet Version 2 addressing scheme.

Ensure that the multicast address is correct. Incorrect addresses can cause network problems. You can enter up to 256 multicast MAC addresses.

Required: Yes

Dependencies: When you select "Enable Additional Multicast Addresses" on page 5-7, you must configure this parameter at least one time.

Valid Values: X'B000 0000 0000' to X'BFFF FFFF FFFF'

Default Value: None

EIA 422/449 Serial Adapter and V.35/V.36 Serial Adapter

Use the worksheet on page A-21.

The EIA 422/449 Serial Adapter and V.35/V.36 Serial Adapter (referred to collectively in this section as *serial adapters*) provide an interface between the IBM 6611 and a data service unit/channel service unit (DSU/CSU) or high-speed serial converter. Both serial adapters support an aggregated data rate of 2 ports x 1.544 Mbps or 3.088 Mbps. If one of the ports is connected to a telecommunications line that provides a data rate of 2.048 Mbps, the maximum rate at which the second port can operate is the residual data rate (3.088—2.048 Mbps).

You must configure “Data Encoding” on page 5-11 when you want to use these adapters. Data encoding must match the encoding used by other routers on the network.

After you configure the serial adapter’s parameters, configure the protocols that you want the adapter to transmit and receive.

The ports on the serial adapters are identified in reverse order. Port number 2 is the closer port from the 6611 planar board. Port number 1 is the further port from the 6611 planar board.

Restrictions: None

Compatible Protocols: The serial adapters support the following protocols:

- For framing data at the physical layer:
 - Frame relay
 - Point-to-Point Protocol (PPP)
 - Token-Ring Network Bridge Program point-to-point
- For routing:
 - IP
 - IPX
 - XNS
 - DECnet
 - AppleTalk
- For bridging, any protocols including the following:
 - IP
 - IPX
 - XNS
 - DECnet
 - SNA
 - NetBIOS
 - AppleTalk
- For data link switching:
 - NetBIOS
 - APPN
 - SNA.

Data Link Protocol: This parameter indicates the frame encapsulation method used to receive and transmit data through the serial adapters.

Required: Yes

Dependencies: When you select **LAN Bridging Protocol** (IBM Token-Ring Network Bridge Program point-to-point), the serial communications link must connect the serial adapter to a PS/2 workstation that is running the IBM Token-Ring Network Bridge Program Version 2.2. The serial adapters are connected to the communications link via a DSU/CSU or modem.

Valid Values: PPP, Frame Relay, LAN Bridging Protocol

Default Value: None

Physical Interface

Enable Interface: This parameter enables or disables one of the ports on the serial adapter. The adapter has two ports. The parameter value you select for each port is independent of the other port. Enable this parameter for each port when you want the serial adapter port to be active on the network.

When a port is enabled, the Configuration Program uses the values of the serial adapter parameters to initialize the port. When a port is disabled, the parameter values are not used but are retained in the configuration file.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Cylink Serial Number: The serial adapters connect to a data service unit/channel service unit (DSU/CSU). When the DSU/CSU is a Cylink 4201 ACSU that is attached to this Serial port and you want to retrieve the network management data from the Cylink, configure this parameter. This parameter identifies the serial number of the Cylink 4201, which can also be used as its address.

To determine the serial number, refer to the Cylink documentation for instructions about how to display the serial number on the front panel of the 4201 ACSU. Verify that the 4201 ACSU address is the same value as configured in this parameter. Configure this parameter for each port of a serial adapter that attaches to Cylink if additional network management data is needed.

Required: No

Dependencies: To use the EIA 232 S2 serial port for a local or remote (modem) connection to a service terminal, this parameter must not be configured.

To use the EIA 232 S2 serial port to retrieve a Cylink serial connection, the data rate must be set to 2400 bps. See "Baud Rate for S2 Serial Port" on page 4-4 for information about configuring the EIA 232 S2 port.

Valid Values: 0 to 99999999

Default Value: None

Serial Line Speed: This parameter should match the clock rate provided by the DSU/CSU. When multiple clock rates are provided, enter the lowest clock rate. It is used internally by the IBM 6611 to determine the length of internal queues.

Required: No

Dependencies: None

Valid Values: 19200 to 204800 bps

Default Value: 19200 bps

Data Encoding: This parameter defines the data encoding method you want to use on the serial communications link that is connected to a port on the serial adapter. Configure this parameter for each port on a serial adapter that you want to use.

Select **NRZ** when you want the serial link to use non-return-to-zero encoding. When NRZ is selected, the signal level on the serial link changes with each transmission of a 0 or a 1. NRZ is a common setting for modems. It determines that a line transition occurs for each zero bit. The transition occurs at the start of the data bit cell. A one is represented by a continuous level.

Select **NRZI** when you want the serial link to use non-return-to-zero-inverted change-on-zeros (NRZI-0) encoding. When **NRZI** is selected, the signal level on the serial link inverts whenever a 0 is encountered. The transition in the signal level occurs at the start of the bit cell. A 1 is represented by no change in the signal.

Required: No

Dependencies: None

Valid Values: NRZI, NRZ

Default Value: NRZI

Locally Administered MAC Address: This parameter makes routing decisions for IPX and XNS over PPP. It is used for all protocols over frame relay. Frame relay uses the serial link as a broadcast interface. With frame relay, all frame relay stations must have a unique MAC address if they are to operate correctly.

Required: Yes

Dependencies: This parameter is required when configuring IPX or XNS.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

LAN Bridging Protocol

Use the worksheet on page A-21.

A serial line attached to a serial adapter port on the IBM 6611 is used to communicate with the IBM Token-Ring Network Bridge Program that is operating on a PS/2 workstation, attached to the other end of a serial line.

Restrictions: This protocol runs only on a serial line attached to an EIA 422/449 Serial Adapter or a V.35/V.36 Serial Adapter port on the IBM 6611. Frame Relay and PPP cannot be configured on the same serial adapter port when this protocol is selected.

Enable LAN Bridging Protocol on this Port: This parameter enables or disables the IBM Token-Ring Network Bridge point-to-point protocol on a serial adapter port.

Required: No

Dependencies: This parameter is enabled when "Data Link Protocol" on page 5-9 is configured to Token-Ring Network Bridge point-to-point.

Valid Values: Enable, Disable

Default Value: Enable

Auto Reboot on Error: This parameter indicates whether the IBM Token-Ring Network Bridge Program point-to-point protocol (running on the PS/2 workstation attached via the serial line to this serial adapter port) automatically restarts to recover from an error that terminates the program. Such errors include an adapter check error or a critical resource depletion error.

Required: No

Dependencies: None

Valid Values: Reboot, Do not reboot

Default Value: Reboot

Performance Counter Threshold: This parameter counts the number of frames per 10000 that the bridge (on a PS/2 workstation, attached to this serial port via a serial line) received and was unable to forward in 1 minute due to a target ring inoperative state, adapter congestion, or an invalid frame. Each unit is 0.01% of the frames not forwarded.

Required: No

Dependencies: None

Valid Values: 0 to 9999

Default Value: 10

Telecommunications Link Error Threshold: This parameter represents the maximum number of frames that are not forwarded per 10000 through the bridge (on a PS/2 workstation, attached to this serial port via a serial line) due to errors on the telecommunications link. This ratio represents the number of frames per 10000 that

are lost on the link. Each unit is 0.01% of frames not forwarded. If this parameter is set to 0, the default threshold is used.

Note: 0 means use the default value provided by the Token-Ring Network Bridge Program point-to-point protocol.

Required: No

Dependencies: None

Valid Values: 0 to 9999

Default Value: 0

Memory Dump on Error: This parameter identifies the disk drive (on the PS/2 workstation attached to the serial adapter via a serial line) that is used to write a memory dump when the program is terminated by an internal programming error. If set to 0, the default drive is used.

Required: No

Dependencies: None

Valid Values: Default drive, A Drive, B Drive, C Drive, D Drive

Default Value: Default drive

Event Log Drive: This parameter identifies the disk drive (on the PS/2 workstation attached to the serial port via a serial line) that is used to write a message indicating the error that caused the bridge program to terminate. When set to 0, the message is written to the default drive.

Required: No

Dependencies: None

Valid Values: Default drive, A Drive, B Drive, C Drive, D Drive

Default Value: Default drive

Largest Frame Size: This parameter identifies the size of the largest frame that the bridge (on the PS/2 workstation, attached to the serial adapter port via a serial line) forwards.

Required: No

Dependencies: None

Valid Values: 516, 1500, 2052 bytes

Default Value: 2052 bytes

Network Management Parameters

Enable Ring Parameter Server: This parameter enables or disables the ring server functions for the IBM Token-Ring Network Bridge Program.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Enable Ring Error Monitor: This parameter enables or disables the ring error monitor functions for the IBM Token-Ring Network Bridge Program.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Enable Configuration Report Saver: This parameter enables or disables the configuration report server functions for the IBM Token-Ring Network Bridge Program.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Passwords to Link Network Managers

Link Password 0: This parameter identifies the link password that is used to secure the reporting links that the LAN network manager makes with the bridge to set parameters and obtain network management information. When the network manager gives a password that is not valid to establish a reporting link, the bridge rejects the reporting link request and notifies any other network manager programs with reporting links. Leave this parameter blank when no password is to be used.

Required: No

Dependencies: None

Valid Values: Six to 8 alphanumeric characters when configured or blank when a password is not used

Default Value: X'0000 0000'

Link Password 1: This parameter identifies the link password that is used to secure the reporting links that the network managers make with the bridge to set parameters and obtain network management information. When a network manager gives a password that is not valid to establish a reporting link, the bridge rejects the reporting link request and notifies any other network manager programs with reporting links. Leave this parameter blank when a password is not used.

Required: No

Dependencies: None

Valid Values: Six to 8 alphanumeric characters when configured or blank when a password is not used

Default Value: X'0000 0000'

Link Password 2: This parameter identifies the link password that is used to secure the reporting links that the network managers make with the bridge to set parameters and obtain network management information. When a network manager gives a password that is not valid to establish a reporting link, the bridge rejects the reporting link request and notifies any other network manager programs with reporting links. Leave this parameter blank when a password is be used.

Required: No

Dependencies: None

Valid Values: Six to 8 alphanumeric characters when configured or blank when a password is not used

Default Value: X'0000 0000'

Link Password 3: This parameter identifies the link password that is used to secure the reporting links that the network managers make with the bridge to set parameters and obtain network management information. When a network manager gives a password that is not valid to establish a reporting link, the bridge rejects the reporting link request and notifies any other network manager programs with reporting links. Leave this parameter blank when a password is not used.

Required: No

Dependencies: None

Valid Values: Six to 8 alphanumeric characters when configured or blank when a password is not used

Default Value: X'0000 0000'

Point-to-Point Protocol (PPP)

Use the worksheet on page A-21.

Point-to-Point Protocol (PPP) defines transmission data over a serial link through an EIA 422/449 Serial Adapter or a V.35/V.36 Serial Adapter port. To configure PPP, you must do the following:

- Enable or disable PPP on each serial adapter port. The default value is set to **Enable**.
- Tailor the parameters by modifying the default values for the other parameters to match your specific network configuration.

Restrictions: PPP can be configured only for a serial adapter port.

Enable Point-to-Point Protocol (PPP) on This Port: This parameter enables or disables PPP on this serial adapter port.

Required: No

Dependencies: This parameter is required when "Data Link Protocol" on page 5-9 is set to **PPP**.

Valid Values: Enable, Disable

Default Value: Disable

Maximum Receive Unit: The maximum receive unit defines the maximum number of octets per packet that are expected to be received on the attached serial line.

Required: No

Dependencies: The IBM 6611 must always be configured to receive a packet of at least 1500 octets (matches Ethernet MTU).

Valid Values: 1500 to 2052 octets

Default Value: 1500 octets

Enable Link Quality Monitoring: This parameter enables or disables link quality monitoring on the line attached to this port. When enabled, link quality is monitored by counting the number of transmitted and received packets and octets. The values are sent to the remote router in intervals to compare the actual values to the expected values. Link quality monitoring enables the IBM 6611 to determine when network traffic should be stopped due to quality problems. Through the link control protocol link reestablishment when the link quality is again acceptable, network traffic will be allowed to resume.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Link Quality Monitoring Interval: This parameter sets the maximum period of time allowed between Link Quality Reports (LQRs). The report is transmitted to the peer router. LQRs continue to be sent when the link is unsuitable for network layer traffic.

Required: No

Dependencies: This parameter is configured when “Enable Link Quality Monitoring” on page 5-16 is enabled.

Valid Values: 1 to 1800 seconds (30 minutes)

Default Value: 30 seconds

Frame Relay

Use the worksheet on page A-21.

Frame relay can be configured only on the EIA 422/449 Serial Adapter or V.35/V.36 Serial Adapter ports. The frame relay configuration of each port of the serial adapter is independent of the other port. This means that another protocol, such as PPP, can be configured on one port and frame relay on the other. The frame relay parameters can be different and independent on each port.

To configure frame relay, perform the following tasks:

- Optionally, you can enter the data link connection identifiers (DLCIs) in “DLCIs Assigned to This Port” on page 5-20 that are provided by the frame relay service provider for the link attached to the serial adapter port that is being configured to use frame relay.
- Tailor the serial adapter port to the service offered by the provider of your frame relay network. These additional parameters are optional and a default value is provided.

Restrictions: Depending on the configuration of frame relay, you may need to provide additional information when configuring the protocols and bridging that will be transported by frame relay.

If the router at the other end of the DLCI does not support the Inverse Address Resolution Protocol (InARP), then you must equate the protocol address of the remote router for each DLCI. See “Use Inverse ARP to Resolve Remote Protocol Addresses” on page 5-20. Refer to the *IBM 6611 Network Processor Introduction and Planning Guide* for more information about frame relay.

Compatible Protocols: The following protocols are routed or bridged over the serial adapter port when configured for frame relay:

- For routing:
 - IP
 - IPX
 - XNS
 - DECnet
 - AppleTalk
- For bridging, any protocols including the following:
 - IP
 - IPX
 - XNS
 - DECnet
 - SNA
 - NetBIOS
 - AppleTalk
- For data link switching:
 - NetBIOS
 - APPN
 - SNA.

Enable Frame Relay on This Port: This parameter enables or disables frame forwarding using frame relay on this port.

When a protocol is enabled, all DLCIs attached to the port are enabled for that protocol unless the DLCIs are listed in the *destination per DLCI* table. In that case, only the DLCIs listed for that protocol are enabled.

Required: No

Dependencies: This parameter is required when “Data Link Protocol” on page 5-9 is set to **Frame Relay**.

Valid Values: Enable, Disable

Default Value: Disable

Polling Interval: This parameter specifies the number of seconds between successive status enquiry messages. The value should be set according to the recommendations of the frame relay service provider.

Required: No

Dependencies: None

Valid Values: 5 to 30 seconds

Default Value: 10 seconds

Full Enquiry Interval: This parameter specifies the number of polling intervals that pass before issuing a full status enquiry message. The default should be changed according to the recommendations of the frame relay service provider.

Required: No

Dependencies: None

Valid Values: 1 to 255

Default Value: 6

LMI Option: This parameter specifies the type of Local Management Interface (LMI) that is active on the frame relay network.

Required: No

Dependencies: None

Valid Values: ANSI T1.617 Annex D, LmiRev1, None

Default Value: ANSI T1.617 Annex D

Use Inverse ARP to Resolve Remote Protocol Addresses: This parameter determines when the protocol addresses of the remote routers that are communicating with this IBM 6611 via frame relay are resolved by using InARP. If you cannot use InARP, you must enter all the network addresses of the remote routers for *each* DLCI provided by the frame relay service provider.

Required: No

Dependencies: None

Note: If AppleTalk is routed on this port, "Use Inverse ARP to Resolve Remote Protocol Addresses" must be enabled.

Valid Values: Enable, Disable

Default Value: Enable

List of DLCI Numbers

DLCIs Assigned to This Port: This parameter defines a list of data link connection identifiers (DLCIs) created by the provider of the frame relay service for the link attached to this serial adapter port. The DLCIs are defined by the frame relay service provider.

This list must be provided when:

- The LMI option is none. The list must include all the DLCIs that are used on the port.
- The LMI option is LmiRev1 or ANSI T1.617 Annex D, and bridging is enabled. The list does not have to include all DLCIs, only those that must have an associated ring number for bridging.
- The LMI option is LmiRev1 or ANSI T1.617 Annex D, and InARP is not supported. The list must contain all DLCIs on the port so that the remote protocol address can be configured.
- LMI option is LmiRev1 or ANSI T1.617 Annex D, and some protocols are to be restricted to specific DLCIs. The list does not have to include all the DLCIs, only those that require configuration modification.

Required: No

Dependencies: This parameter is required to define a list of DLCI numbers.

Valid Values: A valid DLCI (an integer from 1 to 1022)

Default Value: None

SDLC Adapter

Use the worksheet on page A-22.

The SDLC Adapter enables an IBM 6611 to attach to serial communications links that use a CCITT V.35, an EIA 232-D, a CCITT V.24/V.28, or a CCITT X.21 physical interface. Each port can be connected to only one physical interface. The following list and Figure 5-1 specify the interfaces associated with each port:

- Port 0: EIA 232-D, CCITT V.24/V.28, CCITT V.35, or CCITT X.21
- Port 1: EIA 232-D, CCITT V.24/V.28, or CCITT V.35
- Port 2: EIA 232-D or CCITT V.24/V.28
- Port 3: EIA 232-D or CCITT V.24/V.28.

The four ports of the SDLC Adapter are provided by the 6611 SDLC Adapter Interface Cable (*SDLC Adapter Interface Cable*). The single cable connector on the SDLC Adapter is connected to the SDLC Adapter Interface Cable, which has multiple cables and connectors for the supported physical interfaces. Each of the cable connectors on the SDLC Adapter Interface Cable is associated with only one of the four ports. The SDLC Adapter Interface Cable is connected to one or more SDLC Adapter cables, each of which is connected to a serial communications link.

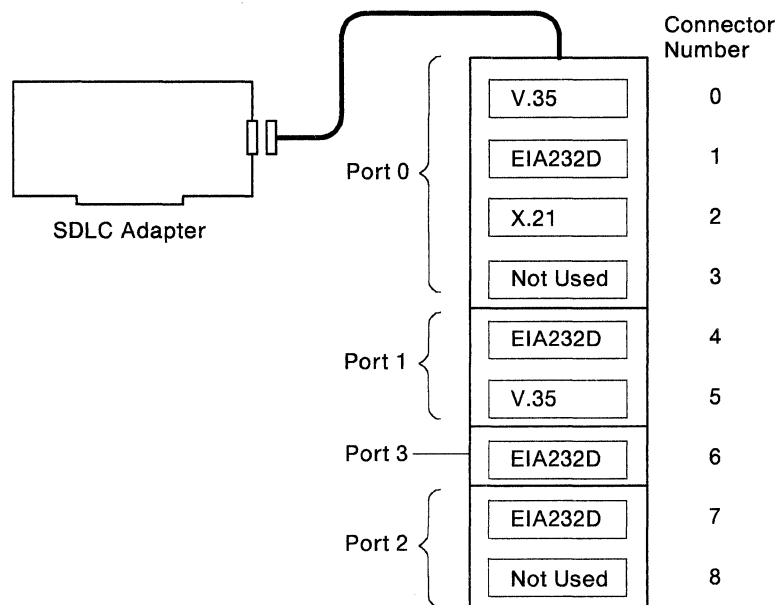


Figure 5-1. SDLC Adapter Ports

The following list specifies the maximum number of connections to the adapter as determined by the type of interface used:

- Four EIA 232-D connections (using ports 0, 1, 2, and 3)
- Four CCITT V.24/V.28 connections (using ports 0, 1, 2, and 3)
- Two CCITT V.35 connections (using ports 0 and 1)
- One CCITT X.21 connection (using port 0)
- Up to four connections of mixed type (using ports 0, 1, 2, and 3).

You must configure at least the following SDLC Adapter configuration parameters when you want to use the adapter:

- Physical link type
- Serial encoding.

After you configure the SDLC Adapter parameters, configure the SDLC Adapter station parameters for each SNA station that will establish sessions with the SDLC Adapter.

Refer to the *IBM 6611 Network Processor Introduction and Planning Guide*.

Restrictions A maximum of three SDLC Adapters can be operated in the IBM 6611 Model 140. A maximum of six SDLC Adapters can be operated in the IBM 6611 Model 170. Only SNA is supported on the SDLC Adapter.

Physical Link Type: This parameter specifies the type of physical interface you can use on this port. Some ports support more than one type of interface, but you can use only one physical interface for each port.

Select the value that corresponds to the physical interface to which this port connects.

- Select **EIA 232-D** when the connection uses the interface defined by Electronic Industries Association (EIA) standard 232-D or CCITT Recommendations V24/V28. This interface is used for directly connecting devices over short distances (less than 60 m [197 ft]) or for connection over long distances using a synchronous modem.
- Select **V.35** when the connection via a DCE to the public telephone network uses the interface defined by the CCITT Recommendation V.35.
- Select **X.21** when the connection is to a DCE that provides a CCITT recommendation X.21 interface. This interface is used to connect to public data networks in many European countries and Japan.

Required: Yes

Dependencies: This parameter is required to configure a serial adapter port. If the port is CCITT V.24/V.28, select EIA 232-D. On the SDLC Adapter interface cable, ports 0, 1, 2, and 3 can be EIA 232-D. Ports 0 and 1 can be V.35. Port 0 can be X.21.

Valid Values: EIA 232-D, V.35, X.21

Default Value: None

Physical Interface

Enable Interface: This parameter enables or disables this port on the SDLC Adapter. Select **Enable** when you want this port to be active on the network.

When the port is enabled, the Multiprotocol Network Program uses the values of the other SDLC Adapter parameters to initialize the port. When the port is disabled, the parameter values are not used but are maintained in the configuration file.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Serial Encoding: This parameter defines the data encoding method you want to use on the serial communications link that is connected to this port of the SDLC Adapter interface cable. Configure this parameter for each port of the SDLC Adapter that you want to use.

Select **NRZ** when you want the serial link to use non-return-to-zero (NRZ) encoding. NRZ is a common setting for use with modems. It determines that a line transition occurs for each zero bit. The transition occurs at the start of the data bit cell. A one is represented by a continuous level.

Select **NRZI** when you want the serial link to use non-return-to-zero-inverted change-on-zeros (NRZI-0) encoding. When **NRZI** is selected, the signal level on the serial link inverts whenever a 0 is encountered. The transition in the signal level occurs at the start of the bit cell. A 1 is represented by no change in the signal.

Required: No

Dependencies: None

Valid Values: NRZ, NRZI

Default Value: NRZ

Data Rate Select: This parameter defines the transmission rate you want to use on the communications line connected to this port.

Select **Full** when you want to use the normal transmission rate of the line connected to this SDLC Adapter port, or when the modem has only one transmission rate.

Select **Alternate** when the modem provides a reduced speed and you prefer to use that speed rather than the speed of the line connected to this port.

Required: No

Dependencies: None

Valid Values: Full, Alternate

Default Value: Full

Request to Send: This parameter determines the manner in which the communications link connected to this port uses the request to send (RTS) signal for attached modems.

Select **Controlled** when you want the RTS signal to be activated with each transmission over this SDLC Adapter port. Select **Continuous** when you want the RTS signal to remain activated as long as the session with this SDLC Adapter port is connected.

Required: No

Dependencies: All stations attached to this port must be compatible with the telecommunications network.

Valid Values: Continuous, Controlled

Default Value: Continuous

Data Terminal Ready: This parameter defines the signal that you want to use on this port of the SDLC Adapter when the IBM 6611 (the data terminating equipment [DTE]) is ready to communicate with the modem (the data circuit-terminating equipment [DCE]) attached to the communications link (line).

Select **Connect data set to line (CDSTL)** when you want the data terminal ready signal (DTR) from the DTE to indicate an unconditional command to the DCE to connect the line to the network or remove the line from the network.

Select **Data terminal ready (DTR)** when you do not want to force the modem to respond to the DTR signal by connecting or removing the line from the network.

Required: No

Dependencies: None

Valid Values: Connect data set to line (CDSTL), Data terminal ready (DTR)

Default Value: Connect data set to line (CDSTL)

SDLC Adapter SNA Stations

Use the worksheet on page A-22.

The SDLC Adapter enables the IBM 6611 to connect to serial communications links that use an EIA 232-D, a CCITT V.24/V.28, a CCITT V.35, or a CCITT X.21 physical interface. Each SNA physical unit (PU) 2.0 station on a port of the SDLC Adapter must be configured. Up to 254 SNA PU 2.0 stations can be configured on a port on the SDLC Adapter. The SDLC Adapter station parameters describe each of these stations.

You must configure at least the following SDLC Adapter station parameters when you want the SNA stations to communicate with the SDLC Adapter:

- "Station Address" on page 5-25
- "Station Token-Ring Source Address" on page 5-25.

The "Station Token-Ring Source Address" on page 5-25 and the "Station Token-Ring Destination Address" on page 5-26 provide token-ring addresses on the virtual token ring that data link switching maintains in the IBM 6611. When "Station Token-Ring Destination Address" on page 5-26 is not configured, the connection to the SNA station occurs when another device that is configured for DLSw provides the token-ring address of this SNA station as the destination token-ring address.

Restrictions: A maximum of 254 SNA stations can be configured for a port on the SDLC Adapter. The values you configure for one station are independent of the values you configure for the other stations and independent of each SDLC port.

List of SNA Stations

Station Address: This parameter specifies the SDLC address of this SNA station. The SDLC address must match the address configured on the station. The SDLC address must be unique on this port.

Required: Yes

Dependencies: This parameter is required to configure SNA stations. This value must be unique on each port.

Valid Values: X'01' to X'FE'

Default Value: None

Station Token-Ring Source Address: When data link switching allows SDLC devices to appear to be attached to a token ring, a token-ring address is needed to address this station at the remote IBM 6611.

Required: Yes

Dependencies: This parameter is required to configure SNA stations. The address must be unique in the IBM 6611.

Valid Values: Any valid locally-administered token-ring MAC address

Default Value: None

Station Token-Ring Source SAP: This parameter defines the SAP when data link switching allows an SDLC device to appear as a token ring.

Required: Yes

Dependencies: None

Valid Values: Any valid locally administered token-ring SNA SAP (X'04' to X'EC')

Default Value: None

Station Token-Ring Destination Address: This parameter defines the token-ring physical address to which this station should be connected. DLSw gives SDLC devices a token-ring appearance. A token-ring physical address is needed to provide connectivity across the remote token-ring network. When an address is entered, the IBM 6611 attempts to connect this station to this parameter's value as soon as this station becomes active. When an address is not entered, the IBM 6611 waits for a remote station to attempt to contact the token-ring address defined in "Station Token-Ring Source Address" on page 5-25 before activating this station.

Required: No

Dependencies: None

Valid Values: Any valid locally-administered token-ring MAC address.

Default Value: None

Station Token-Ring Destination SAP: This parameter defines the token-ring SAP to which this station should be connected.

Required: No

Dependencies: None

Valid Values: Any valid token-ring SNA SAP

Default Value: None

Station XID Value: This parameter defines the XID value that is sent to identify this station.

If this parameter is not configured, the IBM 6611 will attempt to query the station to determine its XID information. Not all stations will respond to this query when defined on a non-switched line. If a station does not respond, this parameter should be configured with the value that the remote device expects which identifies this station.

The contents of this parameter are defined as follows:

Bits	Content
0 – 11	Block number that contains an IBM product specific number. See the product specifications for this station to determine the value to use.
12 – 31	ID number which contains a binary value which is with the block number identifies a specific station uniquely within a network installation. The ID number can be assigned in various ways depending on the product. See the product specification for this station for more information.

Required: No

Dependencies: None

Valid Values: X'0000 0000' to X'FFFF FFFF'

Default Value: None

SNA Station Detail

Primary Slow List Timeout: This parameter defines the amount of time, in seconds, that the primary station, IBM 6611, can wait between polls to secondary stations, SNA PU 2.0 devices, on the slow list. When the primary station detects that all of the frames received from a secondary station are supervisory frames and that the data was not transferred, the primary station adds the secondary station to a slow list. Supervisory frames are used to acknowledge I frames and do not contain data. Therefore, the slow list is a list of secondary stations that are not transferring data.

The primary station polls stations on the slow list less frequently than it does the other secondary stations to avoid using extra network resources with polls. A secondary station is removed from the slow list when it sends an I frame.

Required: No

Dependencies: None

Valid Values: 1 to 60 seconds

Default Value: 1 second

Retransmit Count: This parameter defines the number of information frame errors that can be transmitted in sequence to this station before this station detects that a permanent transmission error occurred. When a permanent transmission error occurs, the station requests that the sender retransmit the I frames.

Required: No

Dependencies: None

Valid Values: 1 to 50 frames

Default Value: 10 frames

Retransmit Threshold: This parameter specifies the number of information frame transmissions that are allowed as a percentage of total number of information frame transmissions. The specified rate is the maximum number of retransmissions allowed over which an error log entry is made.

Required: No

Dependencies: None

Valid Values: 1 to 100 frames

Default Value: 10 frames

Primary Repoll Threshold: This parameter specifies the number of repolls as a percentage of the total number of polls sent to the secondary station. The specified percentage equals the maximum rate of repolls allowed. The IBM 6611 logs a temporary error in its error log when the threshold is exceeded.

Consider these points when determining a value for this parameter:

- Use this value to provide performance information about the link to this station.
- When the value is too low, the error log contains information that does not indicate a link problem. When the value is too high, the error log does not contain any information.

Required: No

Dependencies: None

Valid Values: 1 to 100%

Default Value: 10%

Primary Repoll Count: This parameter specifies the number of times that the primary station polls the secondary station before detecting that the station is not operating. The primary station polls the secondary station and waits for a response from the secondary station.

When the secondary station does not respond within the time specified for the "Primary Repoll Timeout" parameter, the primary station polls the secondary station again. The primary station keeps trying to get a response until the secondary station responds or until the number of retries exceeds the value specified for this parameter. When the number of retries is exceeded, the primary station starts inactivity procedures.

Consider these points when determining a value for this parameter:

- Select a value that reflects the ability of the secondary station to respond in a timely manner.
- When the value is set too low, the primary station may determine that a secondary station is not operating when it is actually busy.
- When the value is set too high, the primary station may wait too long before determining that the secondary station is not operating.

Required: No

Dependencies: None

Valid Values: 3 to 50 times

Default Value: 15 times

Transmit Window Count: This parameter defines the number of SDLC information frames to send to this station before turning the line around to get a response.

Required: No

Dependencies: None

Valid Values: 1 to 7 frames

Default Value: 7 frames

Maximum I-Field Size: This parameter defines the value for the maximum I-field size in octets.

Required: No

Dependencies: None

Valid Values: 265 to 30729 bytes

Default Value: 265 bytes

Force Disconnect Timeout: This parameter defines the number of seconds that the IBM 6611 waits after sending a request to disconnect from the SDLC communications link (a DISC command) before forcing a disconnect.

Required: No

Dependencies: None

Valid Values: 1 to 600 seconds

Default Value: 120 seconds

Primary Repoll Timeout: This parameter defines the length of time that the primary station (IBM 6611) waits for a response from the secondary station (SNA PU 2.0 device). The primary station polls the secondary station and waits for a response from the secondary station. When the secondary station does not respond within the time specified in this parameter, the primary station polls the secondary station again. The primary station continues to poll the secondary station until the secondary station responds or until the number of polls exceeds the value specified by the "Primary Repoll Count" parameter.

Consider these points when determining a value for this parameter:

- Select a value that reflects the ability of the secondary station to respond in a timely manner.
- When the value is set too low, the primary station sends a new poll before the secondary station can respond to the first poll.
- When the value is set too high, the primary station waits too long before determining that the secondary station is not operating.

Required: No

Dependencies: None

Valid Values: 1 to 250 tenths of a second

Default Value: 30 tenths of a second

X.25 Adapter

Use the worksheets on page A-22 and A-23.

The X.25 Adapter allows the IBM 6611 to act as a data terminal equipment (DTE) device. Permanent Virtual Circuits (PVCs) providing continuous connections and Switched Virtual Circuits (SVCs) providing periodic connections are established over the X.25 network.

Restrictions: The X.25 Adapter cannot be configured for bridging. You can configure a maximum of 4 X.25 Adapters per IBM 6611.

Compatible Protocols: The X.25 Adapter can transmit only IP.

SVC Packet Sizes

- No Packet Size Negotiation

“Default SVC Receive Packet Size” on page 5-39 and “Default SVC Transmit Packet Size” on page 5-40 are the default packet sizes to which you subscribe in your X.25 network agreement. These values are used to select the receive and transmit packet sizes for an SVC when packet size negotiation does not take place.

In this case:

- Set “Default SVC Receive Packet Size” on page 5-39 to your default receive packet size for SVCs.
- Set “Default SVC Transmit Packet Size” on page 5-40 to your default transmit packet size for SVCs.
- Set “Receive Packet Size” on page 5-48 to **None**.
- Set “PVC Transmit Packet Size” on page 5-38 to **None**.
- Set “Packet Size Negotiation Facility” on page 5-41 to **Disable**.
- “Packet Size and Packet Window Size Negotiation” on page 5-42 is not applicable.

- Packet Size Negotiation

When you have subscribed to packet size negotiation, which is an optional facility supported by some networks, “Receive Packet Size” on page 5-48 and “PVC Transmit Packet Size” on page 5-38 are used as follows:

1. Incoming calls

The IBM 6611 negotiates or validates packet size values included in incoming calls depending on “Packet Size and Packet Window Size Negotiation” on page 5-42.

Validate means that an incoming value for packet size is accepted when it is less than or equal to the value for “Receive Packet Size” on page 5-48 or “PVC Transmit Packet Size” on page 5-38 as applicable. The call is cleared otherwise.

Negotiate means that an incoming value for packet size is negotiated down in the call accepted packet when it is greater than the value for “Receive Packet Size” on page 5-48 or “PVC Transmit Packet Size” on page 5-38 as applicable.

2. Outgoing calls

“PVC Transmit Packet Size” on page 5-38 and “Receive Packet Size” on page 5-48 are the values that are requested in outgoing calls.

When your network supports packet size negotiation and you have subscribed to this facility:

- Set “Default SVC Receive Packet Size” on page 5-39 to your default receive packet size for SVCs.
- Set “Default SVC Transmit Packet Size” on page 5-40 to your default transmit packet size for SVCs.
- Set “Receive Packet Size” on page 5-48 to your negotiation receive packet size.
- Set “PVC Transmit Packet Size” on page 5-38 to your negotiation transmit packet size.
- Set “Packet Size Negotiation Facility” on page 5-41 to **Enable**.
- Set “Packet Size and Packet Window Size Negotiation” on page 5-42 to negotiate or validate.

SVC Packet Window Sizes

- No Packet Window Size Negotiation

“Default SVC Receive Packet Window Size” on page 5-40 and “Default SVC Transmit Packet Window Size” on page 5-40 are the default packet window sizes to which you subscribed in your X.25 network agreement. These values are used to select the receive and transmit packet window sizes for an SVC when packet window size negotiation does not take place.

In this case,

- Set “Default SVC Receive Packet Window Size” on page 5-40 to your default receive packet window size for SVCs.
- Set “Default SVC Transmit Packet Window Size” on page 5-40 to your default transmit packet window size for SVCs.
- Do not give “Receive Packet Window Size” on page 5-48 a value.
- Do not give “Transmit Packet Window Size” on page 5-48 a value.
- Set “Packet Window Size Negotiation Facility” on page 5-42 to **Disable**.
- “Packet Size and Packet Window Size Negotiation” on page 5-42 is not applicable.

- Packet Window Size Negotiation

When you have subscribed to packet window size negotiation, which is an optional facility supported by some networks, “Receive Packet Window Size” on page 5-48 and “Transmit Packet Window Size” on page 5-48 are used as follows:

1. Incoming calls

The IBM 6611 negotiates or validates packet window size values included in incoming calls depending on “Packet Size and Packet Window Size Negotiation” on page 5-42.

Validate means that an incoming value for packet window size is accepted when it is less than or equal to the value for “Receive Packet

Window Size" on page 5-48 or "Transmit Packet Window Size" on page 5-48 as applicable. The call is cleared otherwise.

Negotiate means that an incoming value for packet window size is negotiated down in the call accepted packet when it is greater than the value for "Receive Packet Window Size" on page 5-48 or "Transmit Packet Window Size" on page 5-48 as applicable.

2. Outgoing calls

"Receive Packet Window Size" on page 5-48 and "Transmit Packet Window Size" on page 5-48 are the values that are requested in outgoing calls.

When your network supports packet window size negotiation and you have subscribed to this facility:

- Set "Default SVC Receive Packet Window Size" on page 5-40 to your default receive packet window size for SVCs.
- Set "Default SVC Transmit Packet Window Size" on page 5-40 to your default transmit packet window size for SVCs.
- Set "Receive Packet Window Size" on page 5-48 to your negotiation receive packet window size.
- Set "Transmit Packet Window Size" on page 5-48 to your negotiation transmit packet window size.
- Set "Packet Window Size Negotiation Facility" on page 5-42 to **Enable**.
- Set "Packet Size and Packet Window Size Negotiation" on page 5-42 to **Negotiate** or **Validate**.

Enable X.25: This parameter enables or disables the X.25 data link connection.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Type of Line: This parameter defines whether the adapter is to be configured as a data terminal equipment (DTE) for normal mode operation, or as a back-to-back DTE for testing.

The normal mode of operation is to have the adapter set to **DTE**. However, two IBM 6611s can be connected back-to-back without an intervening network using a synchronous modem eliminator, or through a pair of synchronous modems. This arrangement is used for testing. In this test arrangement, one IBM 6611 is set to **DTE**, and the other IBM 6611 is set to **Back-to-back DTE**.

Required: No

Dependencies: None

Valid Values: DTE, Back-to-back DTE

Default Value: DTE

Subscription Mapping

Local DTE Address (NUA): This parameter defines the address of the local data terminal equipment (DTE), or network user address (NUA). Do not include a subaddress (suffix).

Most public networks follow CCITT Recommendation X.121 to create DTE addresses. Private networks sometimes use their own scheme for assigning DTE addresses.

Required: Yes

Dependencies: None

Valid Values: 1 to 15 decimal digits

Default Value: None

Network Identifier: This parameter defines the network to which you want to connect. When none of the listed network identifiers correspond to your network name, select **Other public** or **Other private**.

Required: No

Dependencies: None

Valid Values: Datex-P, Datapac, Telenet, DDN, Other Public, Other Private

Default Value: Other Public

Logical Channel Parameters

Lowest LCN for Outgoing SVCs: This parameter defines the lowest-numbered logical channel that can be used for outgoing SVCs. The number depends on your network subscription.

Required: No

Dependencies: The total number of virtual circuits cannot exceed 64, and the highest channel number cannot be greater than 4095.

LCN values must be entered as follows:

- PVC logical channel numbers (LCNs) are less than or equal to SVC incoming LCNs.
- SVC incoming LCNs are less than or equal to SVC 2-way LCNs.
- SVC 2-way LCNs are less than or equal to SVC outgoing LCNs.

Valid Values: 1 to 4095

Default Value: 251

Number of LCNs for Outgoing SVCs: This parameter defines the number of logical channels that can be used for outgoing SVCs. The number depends on your network subscription.

Required: No

Dependencies: The LCNs for incoming SVCs, two-way SVCs, outgoing SVCs, and PVCs must not overlap. The total number of virtual circuits cannot exceed 64, and the highest channel number cannot be greater than 4095.

Valid Values: 0 to 64

Default Value: 0

Lowest LCN for Two-Way SVCs: This parameter defines the lowest-numbered logical channel that can be used for two-way SVCs. The number depends on your network subscription.

Required: No

Dependencies: The total number of virtual circuits cannot exceed 64, and the highest channel number cannot be greater than 4095.

LCN values must be entered as follows:

- PVC LCNs are less than or equal to SVC incoming LCNs.
- SVC incoming LCNs are less than or equal to SVC 2-way LCNs.
- SVC 2-way LCNs are less than or equal to SVC outgoing LCNs.

Valid Values: 1 to 4095

Default: 10

Number of LCNs for Two-Way SVCs: This parameter identifies the number of logical channels that can be used for two-way SVCs. The number depends on your network subscription. The total number of virtual circuits for this adapter must not exceed 64.

Required: No

Dependencies: The LCNs for incoming SVCs, 2-way SVCs, outgoing SVCs, and PVCs must not overlap. The total number of virtual circuits cannot exceed 64, and the highest channel number cannot be greater than 4095.

Valid Values: 0 to 64

Default Value: 20

Lowest LCN for Incoming SVCs: This parameter defines the lowest-numbered logical channel that can be used for incoming SVCs. The number depends on your network subscription.

Required: No

Dependencies: The total number of virtual circuits cannot exceed 64, and the highest channel number cannot be greater than 4095.

LCN values must be entered as follows:

- PVC LCNs are less than or equal to SVC Incoming LCNs
- SVC incoming LCNs are less than or equal to SVC 2-way LCNs
- SVC 2-way LCNs are less than or equal to SVC outgoing LCNs.

Valid Values: 1 to 4095

Default Value: 5

Number of Logical Channels for Incoming SVCs: This parameter defines the maximum number of logical channels that can be used for incoming SVCs. The number depends on your network subscription and must be in the range of 0 to 64.

Required: No

Dependencies: The LCNs for incoming SVCs, two-way SVCs, outgoing SVCs, and PVCs must not overlap. The total number of virtual circuits cannot exceed 64, and the highest channel number cannot be greater than 4095.

Valid Values: 0 to 64

Default Values: 0

Lowest LCN for PVCs: This parameter defines the lowest-numbered logical channel that can be configured as a permanent virtual circuit. The value of this parameter depends on your network subscription.

Required: No

Dependencies: The LCNs for incoming SVCs, two-way SVCs, outgoing SVCs, and PVCs must not overlap. The total number of virtual circuits cannot exceed 64, and the highest channel number cannot be greater than 4095.

Valid Values: 1 to 4095

Default Value: 1

Number of LCNs for PVCs: This parameter defines the number of permanent virtual circuits. The value of this parameter depends on your network subscription.

Required: No

Dependencies: The LCNs for incoming SVCs, two-way SVCs, outgoing SVCs, and PVCs must not overlap. The total number of virtual circuits cannot exceed 64, and the highest channel number cannot be greater than 4095.

Valid Values: 0 to 64

Default Value: 0

Subscription Mapping 2

CCITT Support: This parameter defines the CCITT version of X.25 of your network, either **1980** or **1984**.

Required: No

Dependencies: None

Valid Values: 1980, 1984

Default Value: 1984

Frame Window Size: This parameter defines the window size to use at the frame level. It defines the allowable number of frames to be sent or received before for an acknowledgement is received or sent.

This is the X.25 *k* value.

Required: No

Dependencies: If “Frame Modulo” is set to **8**, the value must be in the range from 1 to 7. If “Frame Modulo” is set to **128**, the value must be in the range from 1 to 127.

Valid Values

- 1 through 7 (frame modulo 8)
- 1 through 127 (frame modulo 128).

Default Value: 7

Frame Modulo: This parameter defines the numbering modulo used by the frame level.

Required: No

Dependencies: None

Valid Values: 8, 128

Default Value: 8

Connection Mode: This parameter defines whether the X.25 Adapter initiates the link-level connection to the DCE (**Active**).

Required: No

Dependencies: None

Valid Values: Active, Passive

Default Value: Active

Auto-Call Options

Auto-Call Unit: This parameter defines the support provided for an auto-call unit. This parameter allows an auto-dial and auto-answer VX32 modem connected to an X.25 line to dial a phone number automatically to accept incoming calls on this line.

The auto-call unit is the VX32 modem supported only on the French Transpac network. It provides a form of X.32 support. For most users, this value is set to **None**. For some Transpac users who desire X.32 support, the appropriate value should be set, depending on whether the system administrator wants to allow all outgoing calls or to prevent incoming calls. It depends on the exact subscription to Transpac.

The following list contains auto-call unit values:

- An auto-call unit set to **None** means you do not initiate the connection automatically.
- An auto-call unit set to **Outgoing calls** means you automatically initiate the connection.

- An auto-call unit set to **Incoming calls** means you automatically receive an incoming call signal at the physical level.
- An auto-call unit set to **Two-way calls** means you can initiate the connection and you can receive an incoming call signal at the physical level.

Required: No

Dependencies: None

Valid Values: None, Outgoing calls, Incoming calls, Two-way calls

Default Value: None

Auto-Call Unit Disconnection Timeout: This parameter defines the number of seconds that elapse between the last call being cleared and the line being disconnected. This parameter applies only when an auto-call unit is attached. The value must be in the range of 0 through 255.

Required: No

Dependencies: This parameter applies when an auto-call unit is attached. 0 means that the line stays connected even when there is no call in progress.

Valid Values: 0 to 255

Default Value: 0

PVC Settings

The following parameters are used to customize a PVC.

List of PVCs

PVC Logical Channel Number: This parameter defines the logical channel number (LCN) of the PVC. The value must be in the range supplied by the network provider.

Required: No

Dependencies: None

Valid Values: The value of “Lowest LCN for PVCs” on page 5-35 to the value of “Lowest LCN for PVCs” on page 5-35 + “Number of LCNs for PVCs” on page 5-35 minus 1.

Default Value: The value of “Lowest LCN for PVCs” on page 5-35.

PVC Receive Packet Size: This parameter is the receive packet size for this PVC.

Required: No

Dependencies: 2048 and 4096 are valid only when “CCITT Support” on page 5-35 is set to **1984**.

Valid Values: 64, 128, 256, 512, 1024, 2048, 4096 bytes

Default Value: 128 bytes

PVC Transmit Packet Size: This parameter defines the transmit packet size for this PVC.

Required: No

Dependencies: 2048 and 4096 are valid only when “CCITT Support” on page 5-35 is set to **1984**.

Valid Values: 64, 128, 256, 512, 1024, 2048, 4096 bytes

Default Value: 128 bytes

PVC Receive Packet Window Size: This parameter defines the receive packet window size for this PVC.

Required: No

Dependencies: None

Valid Values: 1 to 7

Default Value: 2

PVC Transmit Packet Window Size: This parameter is the transmit packet window size for this PVC.

Required: Yes

Dependencies: None

Valid Values: 1 to 7

Default Value: 2

PVC Auto-reset Value: This parameter defines whether a reset packet is sent automatically at PVC startup for the PVC being configured.

Enter 00 if you do not want a reset packet to be sent. Otherwise, enter the non-zero diagnostic code you want to be included in the reset packet.

Required: No

Dependencies: None

Valid Values: Two hexadecimal digits

Default Value: 00

PVC Default Settings

Receive Packet Size: This is the default receive packet size for PVCs.

Required: No

Dependencies: 2048 and 4096 are valid only when “CCITT Support” on page 5-35 is set to 1984.

Valid Values: 64, 128, 256, 512, 1024, 2048, 4096 bytes

Default Value: 128 bytes

Transmit Packet Size: This parameter is the default transmit packet size for PVCs.

Required: No

Dependencies: 2048 and 4096 are valid only when “CCITT Support” on page 5-35 is set to 1984.

Valid Values: 64, 128, 256, 512, 1024, 2048, 4096 bytes

Default Value: 128 bytes

Receive Packet Window Size: This parameter is the default receive packet window size for PVCs.

Required: No

Dependencies: None

Valid Values: 1 to 7

Default Value: 2

Transmit Packet Window Size: This parameter is the default transmit packet window size for PVCs.

Required: No

Dependencies: None

Valid Values: 1 through 7

Default Value: 2

Autoreset Value: This parameter defines if a reset packet is sent automatically at PVC startup.

Enter 00 if you do not want a reset packet to be sent. Otherwise, enter the non-zero diagnostic code to be included in the reset packet.

Required: No

Dependencies: None

Valid Values: Two hexadecimal digits

Default Value: 00

SVC Defaults

Default SVC Receive Packet Size: This parameter defines the default receive packet size for SVCs. The receive packet size can change for an individual call using the optional facilities in the call request packet if you are a subscriber to flow control parameter negotiation.

Required: No

Dependencies: 2048 and 4096 are valid only if “CCITT Support” on page 5-35 is set to 1985.

Valid Values: 64, 128, 256, 512, 1024, 2048, 4096

Default Value: 128

Default SVC Transmit Packet Size: This parameter defines the default transmit packet size for SVCs. The transmit packet size can be changed for an individual call using the optional facilities in the call request packet if you are a subscriber to flow control parameter negotiation.

Required: No

Dependencies: 2048 and 4096 are valid only if “CCITT Support” on page 5-35 is set to 1984.

Valid Values: 64, 128, 256, 512, 1024, 2048, 4096

Default Value: 128

Default SVC Receive Packet Window Size: This parameter defines the default receive packet window size for SVCs. It can be changed for an individual call using the optional facilities in the call request packet if you are a subscriber to flow control parameter negotiation.

Required: No

Dependencies: None

Valid Values: 1 to 7

Default Value: 2

Default SVC Transmit Packet Window Size: This parameter defines the default transmit packet window size for SVCs. It can be changed using the optional facilities in the call request packet if you are a subscriber to flow control negotiation.

Required: No

Dependencies: None

Valid Values: 1 to 7

Default Value: 2

Include Calling Address in Call Request Packets: This parameter defines whether the calling address is included when sending a call request packet.

Required: No

Dependencies: None

Valid Values: Include, Do not include

Default Value: Include

Calling Address in Incoming Call Packets: This parameter determines whether the calling DTE address in an incoming call packet is verified. The incoming call is rejected when a match is not found.

If you configure an * the Incoming Call packets from any remote DTE are accepted, provided that the Incoming Call passes all the other checks.

If you configure a string of decimal digits, the calling address is checked against this string of decimal digits. Placing the “*” at the end of the string indicates that any digits are acceptable in the remainder of the address.

Required: No

Dependencies: None

Valid Values: *, 1 to 14 decimal digits optionally followed by an *, or 15 decimal digits. For example, *,1234*,12345678012345

Default Value: *

Allow Incoming Calls: This parameter defines whether incoming calls are allowed.

Required: No

Dependencies: None

Valid Values: Allow, Forbid

Default Value: Allow

Allow Outgoing Calls: This parameter defines whether outgoing calls are allowed.

Required: No

Dependencies: None

Valid Values: Allow, Forbid

Default Value: Allow

Facilities Control

Packet Size Negotiation Facility: When your network supports this parameter and you are a subscriber to it, select **Enable**. When enabled, the packet size negotiation facility is allowed in call packets. When disabled, calls containing a packet size negotiation facility are cleared.

Required: No

Dependencies: “Packet Size and Packet Window Size Negotiation” on page 5-42 is not applicable when disable is selected for both “Packet Size Negotiation Facility” and “Packet Window Size Negotiation Facility” on page 5-42.

Valid Values: Enable, Disable

Default Value: Enable

Packet Window Size Negotiation Facility: Select **Enable** when your network supports this facility and you are a subscriber. When enabled, the packet window size negotiation facility is allowed in call packets. When disabled, calls containing a packet window size negotiation facility are cleared.

Required: No

Dependencies: "Packet Size and Packet Window Size Negotiation" is not applicable when disable is selected for both "Packet Size Negotiation Facility" on page 5-41 and "Packet Window Size Negotiation Facility."

Valid Values: Enable, Disable

Default Value: Enable

Packet Size and Packet Window Size Negotiation: This parameter defines whether packet sizes and packet window sizes are validated or negotiated when the facilities are present in incoming calls.

Required: No

Dependencies: None

Valid Values: Validate, Negotiate

Default Value: Negotiate

Reverse Charging/Fast Select Facility: This parameter should be set to **Enable** if your network supports this facility, and you are a subscriber to this facility. Reverse charging allows the calling DTE to charge the cost of the calling call to the responding DTE.

If this parameter is set to **Forbid**, all incoming calls requesting reverse charging are cleared.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Allow Reverse Charging: This parameter defines whether reverse charges can be requested in incoming calls. When the reverse charging/fast select facility is present in an incoming call, it specifies whether reverse charging is requested or is not requested. When this parameter is set to **Forbid**, incoming calls requesting reverse charging are cleared.

Required: No

Dependencies: None

Valid Values: Allow, Forbid

Default Value: Allow

Allow Fast Select: This parameter defines whether fast select can be requested in incoming calls. When the reverse charging fast select facility is present in an incoming call, the facility's parameter specifies whether fast select is requested or not requested. When this parameter is set to **Forbid**, incoming calls requesting fast select are cleared. When fast select is set to **Allow**, incoming calls requesting fast select are accepted.

Required: No

Dependencies: None

Valid Values: Allow, Forbid

Default Value: Allow

Closed User Group (CUG) Selection Facility

Basic Format: When your network supports this facility and you are a subscriber to this facility, select **Enable**. When enabled, the basic format CUG selection facility is allowed in call packets. When disabled, calls containing a basic CUG selection facility are cleared.

A closed user group (CUG) permits the DTEs belonging to the group to communicate with each other, but precludes communication with all other DTEs. When the DTE belongs to more than one CUG, one of the CUGs is the preferred CUG. The number of CUGs to which a DTE can belong depends on the network. If the DTE belongs to 99 or fewer CUGs, the basic format (2-digit index) of the CUG selection parameter must be used. If the DTE belongs to between 100 to 9999 CUGs, the extended (4-digit index) format of the CUG selection facility must be used.

Required: No

Dependencies: This parameter is configured only if the CUG with OA facility is to be included in outgoing call request packets.

Valid Values: Enable, Disable

Default Value: Enable

Extended Format: When your network supports this facility and you are a subscriber to this facility, select **Enable**. When enabled, the extended format CUG selection facility is allowed in call packets. When disabled, calls containing an extended format CUG selection facility are cleared.

Required: No

Dependencies: This parameter can be set to **Enable** when "CCITT Support" on page 5-35 is set to 1984.

Valid Values: Enable, Disable

Default Value: Disable

CUG with OA Facility (Basic Format): The CUG with outgoing access (OA) facility permits the DTE to belong to 99 or fewer CUGs and to originate virtual calls to DTEs belonging to other CUGs with the incoming access capability or to DTEs in the open part of the network. When this parameter is disabled, a call containing a CUG with OA selection facility in basic format is cleared.

Required: No

Dependencies: This parameter can be enabled only when "CCITT Support" on page 5-35 is set to 1984.

Valid Values: Enable, Disable

Default Value: Disable

CUG with OA Facility (Extended Format): The extended format CUG with outgoing access (OA) facility permits the DTE to belong to 100 or more CUGs and to originate virtual calls to DTEs belonging to other CUGs with the incoming access capability or to DTEs in the open part of the network. When this parameter is disabled, a call containing a CUG with OA selection facility in extended format is cleared.

Required: No

Dependencies: This parameter can be set to **Enable** when "CCITT Support" on page 5-35 is set to 1984.

Valid Values: Enable, Disable

Default Value: Disable

Closed User Group: This parameter defines the closed user group (CUG) subscription parameter setting. One of the CUGs is the default. A preferred CUG is not specified in the facilities of the call. The value must be on the following values:

- A value of **0** does not allow a closed user group.
- A value of **1** allows a CUG with incoming and outgoing access, without a preferred CUG.
- A value of **2** allows a CUG with incoming access, without a preferred CUG.
- A value of **4** allows a CUG with outgoing access, without a preferred CUG.
- A value of **8** allows a CUG with incoming and outgoing access, with a preferred CUG.
- A value of **16** allows a CUG with incoming access, with preferred CUG.
- A value of **32** allows a CUG with outgoing access, and with a preferred CUG.
- A value of **64** allows a closed user group with a preferred CUG.

Required: No

Dependencies: None

Valid Values: 0, 1, 2, 4, 8, 16, 32, 64

Default Value: 1

X.25 Network Tuning

IP

See "IP Port Parameters" on page 6-51 for information about IP port parameters.

Frame Level Tuning

N2 Counter: This parameter defines the maximum number of times a frame is transmitted under error conditions.

Required: No

Dependencies: None

Valid Values: 1 to 255

Default Value: 20

T1 Timer: This parameter defines the time after which a frame is retransmitted if an acknowledgment is not received.

Required: No

Dependencies: None

Valid Values: 1 to 255

Default Value: 60 (represents 3 seconds)

T4 Timer: This parameter defines the time, in seconds, after which an RR frame is sent. Frame-level recovery is started if no answer is received within T1 time frame.

Required: No

Dependencies: None

Valid Values: 4 to 255

Default Value: 180 (represents 3 minutes)

Packet Level Tuning

Maximum Number of Clear Packets: This parameter defines the number of clear packets that are sent consecutively before the SVC is considered to have failed. This is the R23 counter.

Required: No

Dependencies: None

Valid Values: 0 to 127

Default Value: 2

Maximum Number of Reset Packets: This parameter defines the number of reset packets that can be sent consecutively before the virtual circuit is considered to have failed. This is the R22 counter.

Required: No

Dependencies: None

Valid Values: 0 to 127

Default Value: 2

T24 Timer: This parameter defines a time frame, in seconds. Within this time frame, a receiver ready (RR) packet must be sent following the transmission of a packet requesting an acknowledgment. A value of zero disables this parameter.

Required: No

Dependencies: None

Valid Values: 0 to 255

Default Value: 180

T25 Timer: This parameter defines the time elapsed, in seconds. Within this time period, if no acknowledgement is received, a packet is retransmitted. This is the packet layer equivalent of the T1 timer. Zero disables this parameter.

Required: No

Dependencies: None

Valid Values: 0 to 255

Default Value: 180

Physical Level Tuning

Startup Counter: This parameter determines the number of tests after which the attempted physical-level connection is marked to have failed. When connecting to the network terminating unit (NTU), DTR is raised and the line's data carrier detect (DCD) and data set ready (DSR) are tested. These active lines indicate that the NTU is ready. After raising DTR, these lines are tested at intervals and this value gives the number of tests after which the attempted connection is considered to have failed.

The formula used to determine the retry period is the value of this parameter + 1, multiplied by the value of "Level Poll Timer," then multiplied by 2.

Required: No

Dependencies: None

Valid Values: 1 to 255

Default Value: 11

Level Poll Timer: This parameter defines the time, that elapses between polls of the physical level.

Required: No

Dependencies: "Startup Counter" is part of the equation that determines the retry period.

Valid Values: 10 to 255

Default Value: 10

IP/X.25 Mapping

This set of parameters creates a list of X.25 remote hosts.

List of X.25 Remote Hosts

Destination IP Address for X.25: This parameter is the destination IP address to map to an X.25 virtual circuit. The destination IP node is also referred to as the *remote host*.

Required: Yes

Dependencies: None

Valid Values: Any valid IP address

Default Value: None

Virtual Circuit Type: This parameter defines the type of virtual circuit to be associated with "Destination IP Address for X.25."

Required: No

Dependencies: None

Valid Values: SVC, PVC

Default Value: SVC

Logical Channel (PVCs only): This parameter identifies the logical channel number of the PVC which is used to communicate with the remote host.

Required: No

Dependencies: None

Valid Values: The valid values range between the value of "Lowest LCN for PVCs" on page 5-35 as the low end of the range and the high end of "Lowest LCN for PVCs" on page 5-35 plus "Number of LCNs for PVCs" on page 5-35 minus 1.

Default Value: 1

Remote DTE Address (SVCs only): This parameter defines the X.25 address of the remote DTE.

Required: Yes

Dependencies: None

Valid Values: 1 to 15 decimal digits

Default Value: None

Optional SVC Parameters

Transmit Packet Size: This parameter defines the transmit packet size for this SVC. This parameter is configured only if you are a subscriber to the flow control parameter negotiation facility.

Required: No

Dependencies: Select a value other than **None** only if the packet size negotiation facility is to be included in outgoing call request packets.

Valid Values: 64, 128, 256, 512, 1024, 2048, 4096, None

Default Value: None

Receive Packet Size: This parameter defines the receive packet size for this SVC. Configure this parameter only if you are a subscriber to the flow control parameter negotiation facility.

Required: No

Dependencies: Select a value other than **None** only if the packet size negotiation facility is to be included in outgoing call request packets.

Valid Values: 64, 128, 256, 512, 1024, 2048, 4096, None

Default Value: None

Receive Packet Window Size: This parameter defines the receive packet window size to be used with the virtual circuit.

Required: No

Dependencies: This parameter is configured only if the packet window size negotiation facility is to be included in outgoing call request packets.

Valid Values: 1 through 31

Default Value: None

Transmit Packet Window Size: This parameter defines the transmit packet window size to be used with the virtual circuit.

Required: No

Dependencies: This parameter is configured only if the packet window size negotiation facility is to be included in outgoing call request packets.

Valid Values: 1 through 31

Default Value: None

User-Defined Facilities: This parameter defines the optional user-defined facilities to be included in the call request packet.

Required: No

Dependencies: This parameter is configured only if additional facilities are to be included in outgoing call request packets.

Valid Values: Up to 16 hexadecimal digits.

Default Value: None

Closed User Group Index: This parameter defines the closed user group (CUG) index. The basic format of a CUG is 2 decimal digits. The extended format of a CUG is 4 decimal digits. The 4-digit format is allowed only when the “CCITT Support” on page 5-35 is set to 1984.

Required: No

Dependencies: This parameter is configured only if the CUG with OA facility is to be included in outgoing call request packets.

Valid Values: 00 through 99 or 0000 through 9999

Default Value: None

Closed User Group with Outgoing Access Index: This parameter defines the index of the CUG with outgoing access. The basic format of a CUG is 2 decimal digits. The extended format of a CUG is 4 decimal digits. The 4-digit format is allowed only when “CCITT Support” on page 5-35 is set to 1984.

Required: No

Dependencies: None

Valid Values: 00 through 99, 0000 through 9999

Default Value: None

RPOA Indices: This parameter defines the data network identification code or codes identifying requested RPOA transit networks. Each RPOA index consists of 4 digits. Up to 10 RPOA indices may be specified.

Required: No

Dependencies: This parameter is configured only if one or more RPOAs are to be included in the outgoing call request packets.

Valid Values: Up to 10 indices; each index is 4 decimal digits.

Default Value: None

Chapter 6. Protocol Configuration Parameters

About this Chapter	6-3
Which Protocols Does Each Adapter Support?	6-4
How Does the IBM 6611 Work?	6-4
Source Route Bridging Port Parameters	6-5
List of Ring Number to Frame Relay DLCI Numbers	6-5
Spanning Tree Port Parameters	6-6
Source Route Bridge Filters	6-8
Defining the Order of Port Filters	6-8
Inbound MAC Address Filters	6-9
List of Inbound MAC Address Filters (Source — Destination)	6-9
Inbound Source SAP Filters	6-10
List of Inbound Source SAP Filters	6-11
Inbound SNAP Value Filters	6-11
List of Inbound Source SNAP Filters	6-12
Inbound Ring Number Filters	6-12
List of Inbound Ring Number Filters	6-13
Inbound Sliding Window Filters	6-13
List of Inbound Sliding Window Filters	6-14
Inbound Filter Order	6-16
Outbound MAC Address Filters	6-18
List of Outbound MAC Address Filters	6-19
Outbound Source SAP Filters	6-20
List of Outbound Source SAP Filters	6-21
Outbound SNAP Value Filters	6-21
List of Outbound Source SNAP Filters	6-21
Outbound Ring Number Filters	6-22
List of Outbound Ring Number Filters	6-23
Outbound Sliding Window Filters	6-23
List of Outbound Sliding Window Filters	6-24
Outbound Filter Order	6-25
Hop Count Filter	6-27
Transparent Bridging Port Parameters	6-29
List of Frame Relay DLCIs for Transparent Bridge	6-30
Transparent Bridge Filters	6-32
Defining the Order of Port Filters	6-32
Maximum Transmission Unit Size	6-33
Inbound MAC Address Filters	6-33
List of Inbound MAC Address Filters	6-33
Inbound Source SAP Filters	6-35
List of Inbound Source SAP Filters	6-35
Inbound Ethernet Type Filters	6-36
List of Inbound Ethernet Type Filters	6-36
Inbound Sliding Window Filters	6-37
List of Inbound Sliding Window Filters	6-38
Inbound Filter Order	6-39
Outbound MAC Address Filters	6-41
List of Outbound MAC Address Filters	6-41
Outbound Source SAP Filters	6-43
List of Outbound Source SAP Filters	6-43
Outbound Ethernet Type Filters	6-43
List of Outbound Ethernet Type Filters	6-44
Outbound Sliding Window Filters	6-45

List of Outbound Sliding Window Filters	6-45
Outbound Filter Order	6-47
SNA Port Parameters	6-49
List of SAP Values for Frame Forwarding	6-49
NetBIOS Port Parameters	6-50
IP Port Parameters	6-51
IP Port Filters	6-52
List of IP Port Filters	6-53
IP Destinations Per DLCI	6-55
AppleTalk Port Parameters	6-57
Network Number Ranges	6-57
AppleTalk Ports	6-57
Network Zone Lists	6-57
AppleTalk Port Filters	6-58
User Restrictions on Routing	6-58
Configuration Options	6-58
Define Port Characteristics	6-60
Define Additional Zone Names for Network Zone List	6-62
Define AppleTalk Filters for the Port	6-62
List of Network Number Ranges	6-63
Define DLCI Numbers for Frame Relay Connection	6-64
Restrict Routing to Selected Networks Only	6-64
List of Selected Networks	6-65
Filter Traffic to and from Selected Networks	6-65
List of Network Number Ranges	6-66
Define Allowable Zones for Selected Networks	6-66
IPX Protocol Port Parameters	6-68
IPX Destinations Per DLCI	6-69
IPX Port Filters	6-69
List of IPX Port Filters	6-70
Transport Control Attributes	6-71
Destination Attributes	6-71
Source Attributes	6-73
XNS Port Parameters	6-75
XNS Destinations Per DLCI	6-76
XNS Port Filters	6-77
List of XNS Port Filters	6-77
Transport Control Attributes	6-78
Destination Attributes	6-79
Source Attributes	6-80
DECnet Port Parameters	6-82
List of DLCI Numbers to DECnet Destinations	6-83
DECnet Port Filters	6-84
List of Packet Filters	6-84

About this Chapter

This chapter provides information about the protocol parameters for routing, bridging, and data link switching that are supported by the IBM 6611. This chapter is designed as a reference for Chapter 1 and Appendix A.

Each parameter contains the following information:

Parameter Name	Provides the name of the parameter.
Description	Provides the function of the parameter.
Required	Tells you whether the parameter must be configured to complete the configuration.
Dependencies	Tells you about any related parameters that can affect the way this parameter is configured.
Valid Values	Provides the range of values that can be used.
Default Value	Provides the preset value in the Configuration Program.

Which Protocols Does Each Adapter Support?

Whether an IBM 6611 adapter supports a given protocol depends partly on the compatibility of its addressing scheme and the framing technique. The Token-Ring Network 16/4 Adapter and the Ethernet Adapter support IEEE 802.2 LLC frames and Sub-Network Access Protocol (SNAP) extensions to the IEEE 802 LAN standards.

Table 6-1 indicates the protocols supported by each IBM 6611 adapter.

Table 6-1. IBM 6611 Adapters and Supported Protocols

Adapters:	Ethernet			Token-Ring Network 16/4		EIA 422/449 Serial Adapter and V.35/V.36 Serial Adapter			SDLC	X.25
Standard:	Ver 2	IEEE 802.3		IEEE 802.5						CCITT X.25
Framing:	Type	LLC	SNAP	LLC	SNAP	PPP	Frame Relay	Token-Ring Bridge PPP	SDLC	X.25
Protocols:										
IP	X		X		X	X	X	X		X
XNS	X	X	X	X	X	X	X	X		
IPX	X	X	X	X	X	X	X	X		
DECnet	X		X		X	X	X	X		
SNA	X ¹		X ¹	X		X ¹	X ¹	X ¹	X	X ¹
NetBIOS	X ¹		X ¹	X		X ¹	X ¹	X ¹		X ¹
AppleTalk			X		X	X	X	X		
Transparent Bridging	X	X	X			X	X			
Source Route Bridging				X	X	X	X	X		

¹: Support for NetBIOS and SNA via the EIA 422/449 Serial Adapter, the X.25 Adapter, the Ethernet Adapter and the V.35/V.36 Serial Adapter requires that IP be configured for the adapter port. For those adapters, SNA and NetBIOS are encapsulated in IP datagrams.

How Does the IBM 6611 Work?

The IBM 6611 does not perform protocol conversion. It uses the packet or frame format prescribed by the protocol when it routes or bridges the protocol. The data link switching function encapsulates SNA and NetBIOS frames into an IP datagram for transport across a WAN, but the IBM 6611 does not use encapsulation as a method of transporting other protocols.

Source Route Bridging Port Parameters

Use the worksheet on page A-24.

These parameters are configured for source route bridging on a port.

Enable Source Route Bridging on This Port: This parameter enables or disables source route bridging on this port. When source route bridging is disabled, the configuration information for this port is retained.

Required: No

Dependencies This parameter is configured for a token-ring adapter port, or serial adapter port that is not configured for frame relay or a unique protocol address for each data link connection identifier (DLCI).

Valid Values: Enable, Disable

Default Value: Disable

Ring Number: The bridge number uniquely identifies the network segment or ring within the bridged token-ring network that is directly attached to this port.

Required: Yes

Dependencies: None

Valid Values: X'001' to X'FFE'

Default Value: None

List of Ring Number to Frame Relay DLCI Numbers

The following parameter define the DLCI numbers for the specified ring number.

Ring Number: This parameter uniquely identifies a network segment or ring within the bridged token-ring network that is directly attached to this port.

Required: Yes

Dependencies: None

Valid Values: X'001' to X'FFE'

Default Value: None

DLCI: This parameter displays the DLCI number which is assigned a ring number in "Ring Number."

Required: Yes

Dependencies: This parameter is required to configure a DLCI for a ring number.

Valid Values: A valid DLCI value

Default Value: Current Value

Maximum Transmission Unit: This parameter configures the largest frame size for frames bridged using source route bridging on this port.

Required: No

Dependencies: None

Valid Values: The following table contains the valid values, in bytes:

For a Token-Ring Network 16/4 Adapter (4 MB) Port:	516, 1500, 2052, 4472
For a Token-Ring Network 16/4 Adapter (16 MB) Port:	516, 1500, 2052, 4472, 8144, 11 407, 17 800
For an EIA 422/449 Serial Adapter or a V.35/V.36 Serial Adapter Port:	516, 1500, 2052

Default Value: 2052 bytes

Spanning Tree Port Parameters

Spanning Tree Mode: This parameter determines whether the forwarding of spanning tree explorer frames through the bridge is done automatically by the spanning tree protocol or is manually configured by the network administrator. When this parameter is set to **Manual**, the network administrator can enable or disable the forwarding of spanning tree explorer packets.

Required: No

Dependencies: If you set this parameter to **Manual**, you can enable or disable "Enable Forwarding of Spanning Tree Explorer Packets" on page 6-7. If you set this parameter to **Automatic**, you can assign the cost for a spanning tree explorer frame by configuring the "Path Cost."

Valid Values: Automatic, Manual

Default Value: Automatic

Path Cost: This parameter represents the cost for a spanning tree explorer frame to pass through this port. This value is used to determine spanning tree routes between any two stations. The recommended value for this parameter is 0. When this value is set to 0, the bridge program can automatically calculate a path cost value for this port using its own formula.

Required: No

Dependencies: This parameter is configured when the "Spanning Tree Mode" is set to **Automatic**.

Valid Values: 0 to 65535

Default Value: 0

Enable Forwarding of Spanning Tree Explorer Packets: This parameter enables or disables the use of explorer packets that follow a network spanning tree, reducing the potential congestion on the network.

Required: No

Dependencies: This parameter is configured when the “Spanning Tree Mode” for this port is set to **Manual**.

Valid Values: Enable, Disable

Default Value: Enable

Source Route Bridge Filters

Use the worksheet on page A-24.

The parameters in this section define the following types of inbound and outbound source route bridge filters:

- MAC address
- Source SAP
- SNAP value
- Ring number
- Sliding window
- Hop count.

The terms *inbound* and *outbound* refer to the direction in which frames are flowing, relative to the IBM 6611. Inbound filters are applied to frames flowing into the IBM 6611 from a transmission link or LAN. Outbound filters are applied to frames flowing out of the IBM 6611 onto a transmission link or LAN.

Defining the Order of Port Filters

The system configuration parameters for source route bridging define the order in which inbound and outbound filters are applied on all source route bridge ports on the IBM 6611. The ordering of filters is done by filter type. The default order is:

1. Hop count filters (inbound)
2. Source SAP filters
3. SNAP value filters
4. Ring number filters
5. MAC address filters
6. Sliding window filters.

The default order can be changed for all source route bridge ports by changing the system configuration parameters described in the section "Port Filter Order" on page 3-6.

If the filter order defined by the system configuration parameters is not appropriate for a specific port, you can change the order in which filters will be applied on that port. "Inbound Filter Order" on page 6-16 describes the parameters used to change the order in which inbound filter types are applied on a port. "Outbound Filter Order" on page 6-25 describes the parameters used to change the order in which outbound filter types are applied on port.

The order in which filters are applied can affect the performance of the transparent bridge. As a rule, filters should be applied in the order in which they are most likely to be effective. The result is that the majority of unwanted traffic is discarded in the shortest amount of time, freeing buffer space to accommodate more traffic. For example, suppose you want to define the following port filters:

- A SNAP value filter to deny all IP frames
- A MAC address filter to deny all frames from a specific MAC address.

In this scenario, IP frames represent the majority of the traffic that must be filtered out. By applying SNAP value filters first, you ensure that the largest percentage of unwanted traffic will be discarded in the shortest amount of time. MAC address filters, in this scenario, should be applied second because this filter type is expected to filter out a smaller percentage of traffic.

Inbound MAC Address Filters

Status of All Defined Inbound MAC Filters on This Port: This parameter enables or disables all inbound MAC address filters that are defined. When no inbound MAC Address filters are defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Filter Type: When this parameter is set to **Permit**, only bridge frames with this destination address are permitted to transit this port. More than one permit filter can be defined. However, you cannot define permit and deny filters on the same port. When a permit filter is defined, all other addresses are denied already. When a deny filter is defined, all other addresses are permitted automatically. A deny filter means that the frame with the address in the filter cannot transit this port, but all other frames can.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

Frame Type: This parameter defines the type of frame to which the SAP filter is applied.

Required: No

Dependencies: None

Valid Values: Single route broadcast, All routes broadcast, Both SRB and ARB

Default Value: Both SRB and ARB

List of Inbound MAC Address Filters (Source — Destination)

The following parameters are configured for each MAC address filter that is defined.

Source Frame Address: This parameter contains the source MAC address that matches the frames to which this filter is applied. When the default mask of all zeros is used, no bits in the MAC address are considered significant.

Required: Yes

Dependencies: This parameter is required to define inbound MAC address filters.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

Destination Frame Address: This parameter contains the destination MAC address that matches frames to which this filter is applied. When the default mask of all zeros is used, the bits in the MAC address are not considered significant.

Required: Yes

Dependencies: None

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

Source Frame Address Mask: This parameter contains the source MAC address mask that indicates which bits of the MAC address in "Destination Frame Address" are considered significant when using the filter. When the default mask of all zeros is used, no bits in the MAC address are considered significant. The mask is interpreted as follows: for every bit equal to one in the mask, the same bit in the MAC address is considered significant.

Required: No

Dependencies: None

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: X'7FFF FFFF FFFF'

Destination Frame Address Mask: This parameter contains the destination MAC address mask that indicates which bits of the MAC address are considered significant when using the filter. When a default mask of all zeros is used, no bits in the MAC address are considered significant. The mask is interpreted as follows: for every bit equal to one in the mask, the same bit in the MAC address is considered significant.

Required: No

Dependencies: None

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: X'FFFF FFFF FFFF'

Inbound Source SAP Filters

Status of All Defined Inbound Source SAP Filters on This Port: This parameter enables or disables all inbound source SAP filters that are defined.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Filter Type: When this parameter is set to **Permit**, only bridge frames with this source SAP are permitted to transit this port. More than one permit filter can be defined. However, you cannot define permit and deny filters on the same port. When a permit filter is defined, all other SAPs are denied already. When a deny filter is defined, all other SAPs are permitted already. A deny filter means that frames with the SAP in the filter cannot transit this port, but all other frames can.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

Frame Type: This parameter defines the type of frame to which the SAP filter is applied.

Required: No

Dependencies: None

Valid Values: Single route broadcast, All routes broadcast, Both SRB and ARB

Default Value: Both SRB and ARB

List of Inbound Source SAP Filters

Source SAP Value: This parameter contains the source route bridging SAP value that matches the SAP value of the frames filtered by the inbound source SAP filter. SAP value 00 and 04 is included in the list. You can select as many values as you want from the list.

Required: Yes

Dependencies: This parameter is required to define each inbound source SAP filter that is defined.

Valid Values: X'00' to X'FE' in increments of 2

Default Value: None

Inbound SNAP Value Filters

The following parameters configure inbound source SNAP filters. A maximum of 32 inbound SNAP filters can be defined on a port. These parameters are not required.

Status of All Defined Inbound SNAP Filters on This Port: This parameter enables or disables all inbound SNAP filters defined. When no inbound SNAP filters are defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Filter Type: When this parameter is set to **Permit**, only bridged frames with this SNAP value are permitted to transit this port. More than one permit filter can be defined, but you cannot define both permit and deny filters on the same port. When a permit filter has been defined, all other SNAP values are then denied.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

List of Inbound Source SNAP Filters

SNAP Value: This parameter contains the SNAP value that matches the SNAP value of all frames to which this filter is applied.

Required: Yes

Dependencies: This parameter is required to define outbound source SNAP filters.

Valid Values: X'0600' to X'FFFF'

Default Value: None

SNAP Value Mask: This parameter defines the mask that is combined with the SNAP value to identify a range of SNAP values to filter.

Required: Yes

Dependencies: None

Valid Values: X'0000' to X'FFFF'

Default Value: X'FFFF'

Inbound Ring Number Filters

These parameters configure inbound ring number filters. They are not required. A maximum of 32 inbound ring filters can be defined on a port.

Status of All Defined Ring Number Filters on This Port: This parameter enables or disables all ring number filters that are defined. When a ring number filter is not defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Filter Type: When this parameter is set to **Permit**, only bridge frames with this source ring number in RI field permitted to transit this port. More than one permit filter can be defined. However, you cannot define both permit and deny filters on the same port because when a permit filter is defined all other source ring numbers are already denied. When a deny filter is defined, all other source ring numbers are

already permitted. A deny filter means that the frames with the ring number in the filter cannot transit this port, but all other frames can.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

Frame Type: This parameter defines the type of frame to which the ring number filter is applied.

Required: No

Dependencies: None

Valid Values: Single route broadcast, All routes broadcast, Both SRB and ARB

Default Value: Both SRB and ARB

List of Inbound Ring Number Filters

These parameters are configured for each ring number filter that is configured.

Ring Number: This parameter contains the ring number that matches the source ring number of all frames to which this filter is applied.

Required: Yes

Dependencies: This parameter is required to define inbound ring number filters.

Valid Values: X'001' to X'FFE'

Default Value: None

Ring Number Mask: This parameter contains the ring number mask that indicates the number of the frame to which this filter is applied. When a default mask of all zeros is used, no bits in the ring number are considered significant. The mask is interpreted as follows: for every bit equal to one in the mask, the same bit in the ring number is considered significant.

Required: Yes

Dependencies: This parameter is required to define inbound ring number filters.

Valid Values: X'001' to X'FFE'

Default Value: X'FFF'

Inbound Sliding Window Filters

A maximum of 16 inbound sliding window filters can be defined on a port. A sliding window filter enables you to create a filter for any portion of an inbound frame. You define the contents of a *window* area (which is a block of bytes) and an appropriate offset value. The filter compares the window you define against a byte area at the same offset in an inbound frame. The result of this comparison is determined by the setting of "Filter Type" on page 6-14.

Status of All Defined Inbound Sliding Window Filters on This Port: This parameter enables or disables all inbound sliding window filters defined for a source route bridge port. When no inbound sliding window filters are defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Filter Type: This parameter specifies how the inbound sliding window filters you define are to be interpreted. When this parameter is set to **Permit**, only frames that contain the sliding window bytes you specify are bridged over this port. All other frames are rejected. When this parameter is set to **Deny** (the default), all frames **except** those that contain the sliding window bytes you specify are bridged over this port. Frames that contain the sliding window bytes you specify are rejected.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

Frame Type: This parameter specifies the type of inbound frame the sliding window filter applies to.

Required: No

Dependencies: None

Valid Values: Single route broadcast, All routes broadcast, Both SRB and ARB

Default Value: Both SRB and ARB

List of Inbound Sliding Window Filters

The following parameters are configured for each sliding window filter that is defined.

Filter Name: This parameter specifies the name of the sliding window filter.

Required: Yes

Dependencies: None

Valid Values: 1 to 16 characters

Default Value: None

Offset Starting Field: This parameter specifies where the sliding window filter should be applied in an inbound frame. When you select **MAC**, the sliding window filter is applied at an offset calculated from the beginning of the Access Control field in the MAC header. When you select **SAP**, the sliding window filter is applied at an

offset calculated from the beginning of the source SAP (SSAP) field in the frame. The size of the offset is determined by the parameter "Offset into Frame" on page 6-15.

Note: The source route bridging frame contains a routing information (RI) field which is variable in length. When **SAP** is specified, the offset is calculated from the beginning of the source SAP field, which is after the variable RI field.

Required: No

Dependencies: None

Valid Values: MAC, SAP

Default Value: MAC

Offset into Frame: This parameter specifies a byte offset used in calculating where the sliding window filter should be applied in an inbound frame.

Required: No

Dependencies: This parameter and "Offset Starting Field" on page 6-14 are used to calculate where the sliding window filter should be applied. "Offset Starting Field" determines the starting point in the frame. The sliding window filter is applied at the offset from this starting point specified by this parameter.

Valid Values: 0 to 2084 bytes

Default Value: 0

Sliding Window Contents: This parameter specifies the contents of the sliding window.

Required: Yes

Dependencies: None

Valid Values: A string of up to 30 hexadecimal bytes. Each byte contains 2 hexadecimal digits (00 to FF). The string must end on a byte boundary.

Default Value: None

Sliding Window Mask: This parameter is a *mask* that identifies the significant bits in the string defined for "Sliding Window Contents." Each bit in the mask corresponds to an identical bit in the sliding window contents. For every bit set to one in the mask, the same bit in the sliding window contents is treated as significant.

When the filter is applied, it compares the significant bits in the sliding window contents against bits in an inbound frame. The bit comparison begins at an offset into the frame defined by the parameters "Offset Starting Field" on page 6-14 and "Offset into Frame." Non-significant bits are ignored by the filter. When a mask of all zeros is used, no bits are considered significant; therefore no filtering occurs on the inbound frame. When a mask of all ones is used (the default), all bits in the sliding window are compared against bits at the defined offset in the inbound frame.

Required: No

Dependencies: None

Valid Values: A string of up to 30 hexadecimal bytes. Each byte contains 2 hexadecimal digits (00 to FF). Any bytes in the mask beyond what is specified for the sliding window contents are ignored. When the mask contains fewer bytes than the number of bytes specified for the sliding window contents, the missing bytes will be treated as zeros and the corresponding bytes in the sliding window contents will not be treated as significant.

Default Value: A string of 30 hexadecimal bytes, each with a value of X'FF'.

Inbound Filter Order

The parameters in this section enable you to change the order in which inbound source route bridge filter types are applied on the port being configured. These parameters override the default filter order set by the system configuration parameters for source route bridging. The default order is:

1. Hop count filters
2. Source SAP filters
3. SNAP value filters
4. Ring number filters
5. MAC address filters
6. Sliding window filters.

To override the default order on a specific port, specify a value for each port filter type parameter. The value indicates the order in which the filter type will be applied to inbound frames. A value of **2**, for example, indicates that the filter type will be applied second. A value must be entered for each available filter type.

Change Order Filters Are Applied on This Port and Override System Settings:

When this parameter is enabled, you can change the order in which inbound filter types are applied on the source route bridge port being configured. The order you specify overrides the order defined by the system configuration parameters for source route bridging.

Note: The order you specify affects **only** inbound source route bridge filter types on the port being configured.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Hop Count Filter: This parameter controls when the inbound hop count filter type is to be applied on the source route bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which inbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 6, where 1 specifies that this filter type should be applied **first**, and 6 specifies that this filter type should be applied **last**.

Default Value: None

Source SAP Filter: This parameter controls when the inbound source SAP filter type is to be applied on the source route bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which inbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 6, where 1 specifies that this filter type should be applied **first**, and 6 specifies that this filter type should be applied **last**.

Default Value: None

SNAP Value Filter: This parameter controls when the inbound SNAP value filter type is to be applied on the source route bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which inbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 6, where 1 specifies that this filter type should be applied **first**, and 6 specifies that this filter type should be applied **last**.

Default Value: None

Ring Number Filter: This parameter controls when the inbound ring number filter type is to be applied on the source route bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which inbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 6, where 1 specifies that this filter type should be applied **first**, and 6 specifies that this filter type should be applied **last**.

Default Value: None

MAC Address Filter: This parameter controls when the inbound MAC address filter type is to be applied on the source route bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which inbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 6, where 1 specifies that this filter type should be applied **first**, and 6 specifies that this filter type should be applied **last**.

Default Value: None

Sliding Window Filter: This parameter controls when the inbound sliding window filter type is to be applied on the source route bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which inbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 6, where 1 specifies that this filter type should be applied **first**, and 6 specifies that this filter type should be applied **last**.

Default Value: None

Outbound MAC Address Filters

The following parameters configure MAC address filters. A maximum of 32 outbound MAC address filters can be defined on a port. These parameters are not required.

Status of All Defined Outbound MAC Address Filters on This Port: This parameter enables or disables all outbound MAC address filters that are defined. When no outbound MAC address filters are defined, this parameters does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Filter Type: When this parameter is set to **Permit**, all filters defined for this bridge permit frames to be bridged.

Required: No

Dependencies: This parameter is configured once for outbound MAC address filters that are defined.

Valid Values: Deny, Permit

Default Value: Deny

Frame Type: This parameter defines the type of frame to which the MAC address filter is applied.

Required: No

Dependencies: None

Valid Values: Single route broadcast, All routes broadcast, Both SRB and ARB

Default Value: Both SRB and ARB

List of Outbound MAC Address Filters

These parameters are configured for each outbound MAC address filter that is defined.

Source Frame Address: This parameter contains the source MAC address that matches frames to which this filter is applied. When the default mask of all zeros is used, bits in the MAC address are not considered significant.

Required: Yes

Dependencies: This parameter is configured for each outbound MAC address filter.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

Destination Frame Address: This parameter defines the destination MAC address that matches frames to which this filter is applied. When the default mask of all zeros is used, bits in the MAC address are not considered significant.

Required: Yes

Dependencies: This parameter is configured for each outbound MAC address filter that is defined.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

Source Frame Address Mask: This parameter contains the source MAC address mask that indicates the bits of the MAC address considered significant when using the filter. When the default mask of all zeros is used, bits in the MAC address are not considered significant. The mask interpretation of this is as follows: for every bit equal to one in the mask, the same bit in the MAC address is considered significant.

Required: No

Dependencies: This parameter is configured for each outbound MAC address filter that is defined.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: X'7FFF FFFF FFFF'

Destination Frame Address Mask: This parameter contains the destination MAC address that indicates which bits of the MAC address are considered significant when using the filter. When the default mask of all zeros is used, bits in the MAC address are not considered significant.

Required: No

Dependencies: This parameter is configured for each outbound MAC address filter that is defined.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: X'FFFF FFFF FFFF'

Outbound Source SAP Filters

A maximum of 128 outbound source SAP filters can be configured. These parameters are optional.

Status of All Defined Outbound Source SAP Filters on This Port: This parameter enables or disables all outbound SAP filters. When no outbound SAP filters are configured, the parameter does not affect configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Filter Type: When this parameter is set to **Permit**, only bridged frames with this source SAP are permitted to transit this port. More than one permit filter can be defined. However, you cannot configure permit and deny filters on the same port. When a permit filter is configured, all other source SAPs are denied automatically. A deny filter means that the frames with the source SAP given in the filter cannot transit this port, but other frames can.

Required: No

Dependencies: This parameter is configured once for all outbound source SAP filters.

Valid Values: Deny, Permit

Default Value: Deny

Frame Type: The outbound SAP filter is applied to the frame type defined by this parameter.

Required: No

Dependencies: This parameter is configured once for all outbound source SAP filters.

Valid Values: Single Route Broadcast, All Routes Broadcast, Both SRB and ARB

Default Value: Both SRB and ARB

List of Outbound Source SAP Filters

Source SAP Value: This parameter contains the SAP value that matches the source SAP value of all frames to which this filter is applied.

Required: Yes

Dependencies: This parameter must be configured for each outbound source SAP filter.

Valid Values: X'02' to X'FE'

Default Value: None

Outbound SNAP Value Filters

A maximum of 32 outbound SNAP filters can be configured on a port. These parameters are not required.

Status of All Defined Outbound SNAP Filters on This Port: This parameter enables or disables all outbound SNAP filters. When no outbound SNAP filters are configured, this parameter does not affect configuration.

Required: No

Dependencies: This parameter is configured once for all outbound SNAP filters.

Valid Values: Enable, Disable

Default Value: Disable

Filter Type: When this parameter is set to **Permit**, only bridged frames with this SNAP value address are permitted to transit this port. More than one permit filter can be configured, but you cannot configure permit and deny filters on the same port. When a permit filter is configured, all other SNAP values are denied already. When a deny filter is configured, all other SNAP values are permitted already. A deny filter means the frames with the SNAP value in the filter cannot transit this port, but all other frames can.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

List of Outbound Source SNAP Filters

SNAP Value: This parameter contains the SNAP value that matches the SNAP value of all frames to which this filter is applied.

Required: Yes

Dependencies: This parameter is configured for each outbound SNAP filter.

Valid Values: X'0600' to X'FFFF'

Default Value: None

SNAP Value Mask: This parameter defines the mask that is combined with the SNAP value to identify a range of SNAP values to filter.

Required: Yes

Dependencies: None

Valid Values: X'0000' to X'FFFF'

Default Value: X'FFFF'

Outbound Ring Number Filters

A maximum of 32 outbound ring number filters can be configured. These parameters are not required.

Status of All Defined Outbound Ring Number Filters on This Port: This parameter enables or disables all outbound ring number filters that are defined. When outbound ring number filters are not defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Filter Type: When this parameter is set to **Permit**, all filters defined for this bridge permit frames to be bridged when the source ring number is in the RI field of the frame. When this parameter is set to **Deny**, all filters defined for this bridge deny frames to be bridged when the source ring number is in the RI field of the frame.

Required: No

Dependencies: This parameter is configured once for all filters.

Valid Values: Deny, Permit

Default Value: Deny

Frame Type: This parameter defines the type of frame to which the MAC address filter is applied.

Required: No

Dependencies: None

Valid Values: Single route broadcast, All routes broadcast, Both SRB and ARB

Default Value: Both SRB and ARB

List of Outbound Ring Number Filters

The following parameters are configured for each outbound ring number for which a filter is defined.

Ring Number: This parameter contains the ring number that matches the ring number of all frames to which this filter applies.

Required: Yes

Dependencies: This parameter is required to define outbound ring number filters.

Valid Values: X'001' to X'FFE'

Default Value: None

Ring Number Mask: This parameter defines the mask that is combined with the ring number to identify a range of ring numbers to filter.

Required: Yes

Dependencies: This parameter is required to define the outbound ring number.

Valid Values: X'000' to X'FFF'

Default Value: X'FFF'

Outbound Sliding Window Filters

A maximum of 16 outbound sliding window filters can be defined on a port. A sliding window filter enables you to create a filter for any portion of an outbound frame. You define the contents of a *window* area (which is a block of bytes) and an appropriate offset value. The filter compares the window you define against a byte area at the same offset in an outbound frame. The result of this comparison is determined by the setting of "Filter Type."

Status of All Defined Outbound Sliding Window Filters on This Port: This parameter enables or disables all outbound sliding window filters defined for a source route bridge port. When no outbound sliding window filters are defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Filter Type: This parameter specifies how the outbound sliding window filters you define are to be interpreted. When this parameter is set to **Permit**, only frames that contain the sliding window bytes you specify are bridged over this port. All other frames are rejected. When this parameter is set to **Deny** (the default), all frames **except** those that contain the sliding window bytes you specify are bridged over this port. Frames that contain the sliding window bytes you specify are rejected.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

Frame Type: This parameter specifies the type of outbound frame the sliding window filter applies to.

Required: No

Dependencies: None

Valid Values: Single route broadcast, All routes broadcast, Both SRB and ARB

Default Value: Both SRB and ARB

List of Outbound Sliding Window Filters

The following parameters are configured for each sliding window filter that is defined.

Filter Name: This parameter specifies the name of the sliding window filter.

Required: Yes

Dependencies: None

Valid Values: 1 to 16 characters

Default Value: None

Offset Starting Field: This parameter specifies where the sliding window filter should be applied in an outbound frame. When you select **MAC**, the sliding window filter is applied at an offset calculated from the beginning of the Access Control field of the MAC header. When you select **SAP**, the sliding window filter is applied at an offset calculated from the beginning of the source SAP (SSAP) field in the frame. The size of the offset is determined by the parameter "Offset into Frame."

Note: The source route bridging frame contains a routing information (RI) field which is variable in length. When **SAP** is specified, the offset is calculated from the beginning of the source SAP field, which is after the variable RI field.

Required: No

Dependencies: None

Valid Values: MAC, SAP

Default Value: MAC

Offset into Frame: This parameter specifies a byte offset used in calculating where the sliding window filter should be applied in an outbound frame.

Required: No

Dependencies: This parameter and "Offset Starting Field" are used to calculate where the sliding window filter should be applied. "Offset Starting Field" determines the starting point in the frame. The sliding window filter is applied at the offset from this starting point specified by this parameter.

Valid Values: 0 to 2084 bytes

Default Value: 0

Sliding Window Contents: This parameter specifies the contents of the sliding window.

Required: Yes

Dependencies: None

Valid Values: A string of up to 30 hexadecimal bytes. Each byte contains 2 hexadecimal digits (00 to FF). The string must end on a byte boundary.

Default Value: None

Sliding Window Mask: This parameter is a *mask* that identifies the significant bits in the string defined for "Sliding Window Contents." Each bit in the mask corresponds to an identical bit in the sliding window contents. For every bit set to one in the mask, the same bit in the sliding window contents is treated as significant.

When the filter is applied, it compares the significant bits in the sliding window contents against bits in an outbound frame. The bit comparison begins at an offset into the frame defined by the parameters "Offset Starting Field" on page 6-24 and "Offset into Frame" on page 6-24. Non-significant bits are ignored by the filter. When a mask of all zeros is used, no bits are considered significant; therefore no filtering occurs on the outbound frame. When a mask of all ones is used (the default), all bits in the sliding window value are compared against bits at the defined offset in the outbound frame.

Required: No

Dependencies: None

Valid Values: A string of up to 30 hexadecimal bytes. Each byte contains 2 hexadecimal digits (00 to FF). Any bytes in the mask beyond what is specified for the sliding window contents are ignored. When the mask contains fewer bytes than the number of bytes specified for the sliding window contents, the missing bytes will be treated as zeros and the corresponding bytes in the sliding window contents will not be treated as significant.

Default Value: A string of 30 hexadecimal bytes, each with a value of X'FF'.

Outbound Filter Order

The parameters in this section enable you to change the order in which outbound source route bridge filter types are applied on the port being configured. These parameters override the default filter order set by the system configuration parameters for source route bridging. The default order for outbound frames is:

1. Source SAP filters
2. SNAP value filters
3. Ring number filters
4. MAC address filters
5. Sliding window filters.

To override the default order on a specific port, specify a value for each port filter type parameter. The value indicates the order in which the filter type will be applied to outbound frames. A value of **2**, for example, indicates that the filter type will be applied second. A value must be entered for each available filter type.

Change Order Filters Are Applied on This Port and Override System Settings:

When this parameter is enabled, you can change the order in which outbound filter types are applied on the source route bridge port being configured. The order you specify overrides the order defined by the system configuration parameters for source route bridging.

Note: The order you specify affects **only** outbound source route bridge filter types on the port being configured.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Source SAP Filter: This parameter controls when the outbound source SAP filter type is to be applied on the source route bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which outbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 6, where 1 specifies that this filter type should be applied **first**, and 6 specifies that this filter type should be applied **last**.

Default Value: None

SNAP Value Filter: This parameter controls when the outbound SNAP value filter type is to be applied on the source route bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which outbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 6, where 1 specifies that this filter type should be applied **first**, and 6 specifies that this filter type should be applied **last**.

Default Value: None

Ring Number Filter: This parameter controls when the outbound ring number filter type is to be applied on the source route bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which outbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 6, where 1 specifies that this filter type should be applied **first**, and 6 specifies that this filter type should be applied **last**.

Default Value: None

MAC Address Filter: This parameter controls when the outbound MAC address filter type is to be applied on the source route bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which outbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 6, where 1 specifies that this filter type should be applied **first**, and 6 specifies that this filter type should be applied **last**.

Default Value: None

Sliding Window Filter: This parameter controls when the outbound sliding window filter type is to be applied on the source route bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which outbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 6, where 1 specifies that this filter type should be applied **first**, and 6 specifies that this filter type should be applied **last**.

Default Value: None

Hop Count Filter

The hop count filter is not required. A maximum of one filter can be defined on a port.

Hop Count: This parameter specifies the maximum hop count allowed for each inbound frame being bridged. When the hop count in the inbound frame is equal to or greater than the value in this field, the frame is discarded.

Required: No

Dependencies: None

Valid Values: 1 to 7

Default Value: 7

Frame Type: This parameter defines the type of frame to which the hop count filter is applied.

Required: No

Dependencies: None

Valid Values: Single route broadcast (SRB), All routes broadcast (ARB), Both SRB and ARB

Default Value: Both SRB and ARB

Transparent Bridging Port Parameters

Use the worksheet on page A-25.

This section describes the parameters for configuring transparent bridging on the following adapters:

- Ethernet Adapter
- EIA 422/449 Serial Adapter
- V.35/V.36 Serial Adapter.

“Transparent Bridging” on page 3-10 describes the system configuration parameters for transparent bridging.

Note: The IBM 6611 supports Ethernet transparent bridging, as defined in the IEEE standard for Media Access Control Bridges (802.1D). The IBM 6611 does not support source routing transparent bridging.

Enable Transparent Bridging on This Port: This parameter enables or disables transparent bridging on this port. When transparent bridging is disabled, the configuration information for this port is retained.

To successfully configure transparent bridging, you also need to enable the transparent bridging function at the system level.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Port Priority: This parameter specifies the priority of the transparent bridge port. The port priority is used to select a *preferred port* when:

- Two or more transparent bridge ports are connected to the same Ethernet segment in a redundant configuration. (The transparent bridge spanning tree will allow a path through only one of the ports.)
- Two or more transparent bridge ports have equal path costs to the root bridge.

If ports have equal priorities, then the port with the lowest port number will be the preferred port. Port numbers are assigned automatically by the IBM 6611.

Required: No

Dependencies: None

Valid Values: X'00' to X'FF', where X'00' is the **highest** priority value and X'FF' is the **lowest** priority value

Default Value: X'80'

Determine Port State Automatically: This parameter specifies whether the port state is determined automatically by the spanning tree algorithm or is manually configured by the network administrator.

When this parameter is disabled, the network administrator can control the forwarding of packets through the bridge by configuring “Port State” on page 6-30.

Required: No

Dependencies: If you disable this parameter, you can manually select the "Port State."

Valid Values: Enable, Disable

Default Value: Enable

Port State: This parameter specifies the state of the port. Select **Forwarding** to have the port permanently participate in frame forwarding. Select **Disabled** to permanently stop the port from forwarding frames.

When this parameter is set to **Forwarding**, it overrides the port state that would have been selected by the spanning tree algorithm. Because the spanning tree algorithm cannot automatically disable this port, the network administrator must ensure that this port does not cause a loop in the network when the port is in the forwarding state.

Required: No

Dependencies: This parameter can be configured only when "Determine Port State Automatically" on page 6-29 is disabled.

Valid Values: Forwarding, Disabled

Default Value: Disabled

Path Cost: This parameter is the contribution of this port to the total cost of the paths to the root bridge. For a value of zero (the default), the path cost is calculated using the formula,

$$1000/\text{media speed (in Mbps)}$$

for the following media types:

<u>Media type</u>	<u>Media speed</u>
Ethernet	10 Mbps
Frame Relay or PPP	0.0192 Mbps (19200 bps) to 1.536 Mbps, depending on the serial line speed configured for the serial adapter.

Required: No

Dependencies: None

Valid Values: 0 to 65535

Default Value: 0 (cost calculated using path cost formula)

List of Frame Relay DLCIs for Transparent Bridge

Use the following parameter to define a list of DLCIs that will be used by the IBM 6611 for remote transparent bridging over a frame relay network. The following parameter appears when you are defining transparent bridging on a serial adapter port configured to support frame relay.

DLCI Number: This parameter identifies a data link connection identifier (DLCI) that will be used to transmit transparent bridge frames over a frame relay network. The parameter displays the list of the DLCIs that have been defined for the port. You must select at least one DLCI from this list to successfully configure transparent bridging on the port.

The frame relay service provider assigns DLCIs for each DTE-to-DTE connection a service requester needs. The IBM 6611 functions as a DTE when defined as part of a frame relay network.

Required: Yes

Dependencies: In order to specify this parameter, you need to first define the list of DLCIs assigned to this serial adapter port. See “DLCIs Assigned to This Port” on page 5-20 for more information.

Valid Values: Any available DLCI in the port list

Default Value: None

Transparent Bridge Filters

In addition to defining the maximum transmission unit size that can be handled by a transparent bridge port, the parameters in this section define the following types of inbound and outbound transparent bridge filters:

- MAC address
- Source SAP
- Ethernet type
- Sliding window.

The terms *inbound* and *outbound* refer to the direction in which frames are flowing, relative to the IBM 6611. Inbound filters are applied to frames flowing into the IBM 6611 from a transmission link or LAN. Outbound filters are applied to frames flowing out of the IBM 6611 onto a transmission link or LAN.

Defining the Order of Port Filters

The system configuration parameters for transparent bridging define the order in which inbound and outbound filters are applied on all transparent bridge ports on the IBM 6611. The ordering of filters is done by filter type. The default order is:

1. Source SAP filters
2. Ethernet Type filters
3. MAC address filters
4. Sliding window filters.

The default order can be changed for all transparent bridge ports by changing the system configuration parameters described in the section “Port Filter Order” on page 3-13.

If the filter order defined by the system configuration parameters is not appropriate for a specific port, you can change the order in which filters will be applied on that port. “Inbound Filter Order” on page 6-39 describes the parameters used to change the order in which inbound filter types are applied on a port. “Outbound Filter Order” on page 6-47 describes the parameters used to change the order in which outbound filter types are applied on port.

The order in which filters are applied can affect the performance of the transparent bridge. As a rule, filters should be applied in the order in which they are most likely to be effective. The result is that the majority of unwanted traffic is discarded in the shortest amount of time, freeing up buffer space to accommodate more traffic. For example, suppose you want to define the following port filters:

- An Ethernet Type filter to deny all IP frames
- A MAC address filter to deny all frames from a specific MAC address.

In this scenario, IP frames represent the majority of the traffic that must be filtered out. By applying Ethernet Type filters first, you ensure that the largest percentage of unwanted traffic will be discarded in the shortest amount of time. MAC address filters, in this scenario, should be applied second because this filter type is expected to filter out a smaller percentage of traffic.

Maximum Transmission Unit Size

The following parameter is configured once for each transparent bridge port.

Maximum Transmission Unit Size: This parameter specifies the size of the largest transmission unit that the transparent bridge can transmit and receive on this port. For an Ethernet Version 2 frame, the transmission unit is the Data field in the frame. For an IEEE 802.3 frame, the transmission unit is the logical link control (LLC) PDU in the frame.

Required: No

Dependencies: None

Valid Values: 128 to 1500 bytes

Default Value: 1500 bytes

Inbound MAC Address Filters

A maximum of 32 inbound MAC address filters can be defined on a port.

Status of All Defined Inbound MAC Address Filters on This Port: This parameter enables or disables all inbound MAC address filters defined for a transparent bridge port. When no inbound MAC address filters are defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Filter Type: This parameter specifies how the inbound MAC address filters you define are to be interpreted. When this parameter is set to **Permit**, only those frames with the MAC addresses you specify are bridged over this port. All other frames are rejected. When this parameter is set to **Deny** (the default), all frames **except** those with the MAC addresses you specify are bridged over this port. Frames containing the MAC addresses you specify are rejected.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

List of Inbound MAC Address Filters

The following parameters are configured for each inbound MAC address filter that is defined.

Source MAC Address: This parameter specifies the source MAC address used in the filter. The filter compares this MAC address against all inbound source MAC addresses. The result of the comparison is determined by the setting of "Filter Type."

Required: Yes

Dependencies: “Source MAC Address Mask” identifies the *significant bits* in the source MAC address defined for this filter.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

Destination MAC Address: This parameter specifies the destination MAC address used in the filter. The filter compares this MAC address against all inbound destination MAC addresses. The result of the comparison is determined by the setting of “Filter Type” on page 6-33.

Required: Yes

Dependencies: “Destination MAC Address Mask” identifies the *significant bits* in the destination MAC address defined for this filter.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

Source MAC Address Mask: This parameter is a *mask* that identifies the significant bits in the source MAC address for the filter. Each bit in the mask corresponds to an identical bit in the source MAC address. For every bit set to one in the mask, the same bit in the MAC address is treated as significant.

When the filter is applied, it compares the significant bits in the source MAC address against the same bits in an inbound source MAC address. Non-significant bits are ignored by the filter. When a mask of all zeros is used, no bits are considered significant; therefore no filtering occurs on inbound source MAC addresses. When a mask of all ones is used (the default), inbound source MAC addresses are compared against the entire source MAC address defined for this filter.

Required: No

Dependencies: None

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: X'FFFF FFFF FFFF'

Destination MAC Address Mask: This parameter is a *mask* that identifies the significant bits in the destination MAC address for the filter. Each bit in the mask corresponds to an identical bit in the destination MAC address. For every bit set to one in the mask, the same bit in the MAC address is treated as significant.

When the filter is applied, it compares the significant bits in the destination MAC address against the same bits in an inbound destination MAC address. Non-significant bits are ignored by the filter. When a mask of all zeros is used, no bits are considered significant; therefore no filtering occurs on inbound destination MAC addresses. When a mask of all ones is used (the default), inbound destination MAC addresses are compared against the entire destination MAC address defined for this filter.

Required: No

Dependencies: None

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: X'FFFF FFFF FFFF'

Inbound Source SAP Filters

A maximum of 128 inbound source SAP filters can be defined on a port.

Status of All Defined Inbound Source SAP Filters on This Port: This parameter enables or disables all inbound source SAP filters defined for a transparent bridge port. When no inbound source SAP filters are defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Filter Type: This parameter specifies how the inbound source SAP filters you define are to be interpreted. When this parameter is set to **Permit**, only those frames with the SAP values you specify are bridged over this port. All other frames are rejected. When this parameter is set to **Deny** (the default), all frames **except** those with the SAP values you specify are bridged over this port. Frames containing the SAP values you specify are rejected.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

List of Inbound Source SAP Filters

The following parameter is configured for each inbound source SAP filter that is defined.

Source SAP Value: This parameter specifies the source SAP value used in the filter. The filter compares this SAP value against all inbound source SAP values. The result of the comparison is determined by the setting of "Filter Type."

Required: Yes

Dependencies: None

Valid Values: X'02' to X'FE' in increments of 2

Default Value: None

Inbound Ethernet Type Filters

A maximum of 32 inbound Ethernet Type filters can be defined on a port. This filter is applied to the contents of the Type field within an Ethernet frame. The Type field identifies the type of data encapsulated within an Ethernet Version 2 frame or IEEE 802.3 frame with a SNAP header.

Status of All Defined Inbound Ethernet Type Filters on This Port: This parameter enables or disables all inbound Ethernet Type filters defined for a transparent bridge port. When no inbound Ethernet Type filters are defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Filter Type: This parameter specifies how the inbound Ethernet Type filters you define are to be interpreted. When this parameter is set to **Permit**, only those frames with the Ethernet Type values you specify are bridged over this port. All other frames are rejected. When this parameter is set to **Deny** (the default), all frames **except** those with the Ethernet Type values you specify are bridged over this port. Frames containing the Ethernet Type values you specify are rejected.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

List of Inbound Ethernet Type Filters

The following parameters are configured for each Ethernet Type filter that is defined.

Ethernet Type Value: This parameter specifies the Ethernet Type value used in the filter. The filter compares this Ethernet Type value against all inbound Ethernet Type values. The result of the comparison is determined by the setting of "Filter Type."

Required: Yes

Dependencies: None

Valid Values: X'0000' to X'FFFF'

Default Value: None

Ethernet Type Mask: This parameter is a *mask* that identifies the significant bits in the Ethernet Type value for the filter. Each bit in the mask corresponds to an identical bit in the Ethernet Type value. For every bit set to one in the mask, the same bit in the Ethernet Type value is treated as significant.

When the filter is applied, it compares the significant bits in the Ethernet Type value against the same bits in an inbound Ethernet Type value. Non-significant bits are ignored by the filter. When a mask of all zeros is used, no bits are considered significant; therefore no filtering occurs on inbound Ethernet Type values. When a mask of all ones is used (the default), inbound Ethernet Type values are compared against the entire Ethernet Type value defined for this filter.

Required: Yes

Dependencies: None

Valid Values: X'0000' to X'FFFF'

Default Value: X'FFFF'

Inbound Sliding Window Filters

A maximum of 16 inbound sliding window filters can be defined on a port. A sliding window filter enables you to create a filter for any portion of an inbound frame. You define the contents of a *window* area (which is a block of bytes) and an appropriate offset value. The filter compares the window you define against a byte area at the same offset in an inbound frame. The result of this comparison is determined by the setting of "Filter Type."

Status of All Defined Inbound Sliding Window Filters on This Port: This parameter enables or disables all inbound sliding window filters defined for a transparent bridge port. When no inbound sliding window filters are defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Filter Type: This parameter specifies how the inbound sliding window filters you define are to be interpreted. When this parameter is set to **Permit**, only frames that contain the sliding window bytes you specify are bridged over this port. All other frames are rejected. When this parameter is set to **Deny** (the default), all frames **except** those that contain the sliding window bytes you specify are bridged over this port. Frames that contain the sliding window bytes you specify are rejected.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

List of Inbound Sliding Window Filters

The following parameters are configured for each sliding window filter that is defined.

Filter Name: This parameter specifies the name of the sliding window filter.

Required: Yes

Dependencies: None

Valid Values: 1 to 16 characters

Default Value: None

Offset Starting Field: This parameter specifies where the sliding window filter should be applied in an inbound frame. When you select **MAC**, the sliding window filter is applied at an offset calculated from the beginning of the frame. When you select **Data**, the sliding window filter is applied at an offset calculated from the beginning of the Data field in the frame. The size of the offset is determined by the parameter "Offset into Frame."

Required: No

Dependencies: None

Valid Values: MAC, Data

Default Value: MAC

Offset into Frame: This parameter specifies a byte offset used in calculating where the sliding window filter should be applied in an inbound frame.

Required: No

Dependencies: This parameter and "Offset Starting Field" are used to calculate where the sliding window filter should be applied. "Offset Starting Field" determines the starting point in the frame. The sliding window filter is applied at the offset from this starting point specified by this parameter.

Valid Values: 0 to 1513 bytes

Default Value: 0

Sliding Window Contents: This parameter specifies the contents of the sliding window.

Required: Yes

Dependencies: None

Valid Values: A string of up to 30 hexadecimal bytes. Each byte contains 2 hexadecimal digits (00 to FF). The string must end on a byte boundary.

Default Value: None

Sliding Window Mask: This parameter is a *mask* that identifies the significant bits in the string defined for “Sliding Window Contents.” Each bit in the mask corresponds to an identical bit in the sliding window contents. For every bit set to one in the mask, the same bit in the sliding window contents is treated as significant.

When the filter is applied, it compares the significant bits in the sliding window contents against bits in an inbound frame. The bit comparison begins at an offset into the frame defined by the parameters “Offset Starting Field” on page 6-38 and “Offset into Frame” on page 6-38. Non-significant bits are ignored by the filter. When a mask of all zeros is used, no bits are considered significant; therefore no filtering occurs on the inbound frame. When a mask of all ones is used (the default), all bits in the sliding window are compared against bits at the defined offset in the inbound frame.

Required: No

Dependencies: None

Valid Values: A string of up to 30 hexadecimal bytes. Each byte contains 2 hexadecimal digits (00 to FF). Any bytes in the mask beyond what is specified for the sliding window contents are ignored. When the mask contains fewer bytes than the number of bytes specified for the sliding window contents, the missing bytes will be treated as zeros and the corresponding bytes in the sliding window contents will not be treated as significant.

Default Value: A string of 30 hexadecimal bytes, each with a value of X'FF'.

Inbound Filter Order

The parameters in this section enable you to change the order in which inbound transparent bridge filter types are applied on the port being configured. These parameters override the default filter order set by the system configuration parameters for transparent bridging. The default filter order is:

1. Source SAP filters
2. Ethernet Type filters
3. MAC address filters
4. Sliding window filters.

To override the default filter order on a specific port, specify a value for each port filter type parameter. The value indicates the order in which the filter type will be applied to inbound frames. A value of **2**, for example, indicates that the filter type will be applied second. A value must be entered for each available filter type.

Change Order Filters Are Applied on This Port and Override System Settings:

When this parameter is enabled, you can change the order in which inbound filter types are applied on the transparent bridge port being configured. The order you specify overrides the order defined by the system configuration parameters for transparent bridging.

Note: The order you specify affects **only** inbound transparent bridge filter types on the port being configured.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Source SAP Filter: This parameter controls when the inbound source SAP filter type is to be applied on the transparent bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which inbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 4, where 1 specifies that this filter type should be applied **first**, and 4 specifies that this filter type should be applied **last**.

Default Value: None

Ethernet Type Filter: This parameter controls when inbound Ethernet Type filters are to be applied on the transparent bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which inbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 4, where 1 specifies that this filter type should be applied **first**, and 4 specifies that this filter type should be applied **last**.

Default Value: None

MAC Address Filter: This parameter controls when the inbound MAC address filter type is to be applied on the transparent bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which inbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 4, where 1 specifies that this filter type should be applied **first**, and 4 specifies that this filter type should be applied **last**.

Default Value: None

Sliding Window Filter: This parameter controls when the inbound sliding window filter type is to be applied on the transparent bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which inbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 4, where 1 specifies that this filter type should be applied **first**, and 4 specifies that this filter type should be applied **last**.

Default Value: None

Outbound MAC Address Filters

A maximum of 32 outbound MAC address filters can be defined on a port.

Status of All Defined Outbound MAC Address Filters on This Port: This parameter enables or disables all outbound MAC address filters defined for a transparent bridge port. When no outbound MAC address filters are defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Filter Type: This parameter specifies how the outbound MAC address filters you define are to be interpreted. When this parameter is set to **Permit**, only those frames with the MAC addresses you specify are bridged over this port. All other frames are rejected. When this parameter is set to **Deny** (the default), all frames **except** those with the MAC addresses you specify are bridged over this port. Frames containing the MAC addresses you specify are rejected.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

List of Outbound MAC Address Filters

The following parameters are configured for each outbound MAC address filter that is defined.

Source MAC Address: This parameter specifies the source MAC address used in the filter. The filter compares this MAC address against all outbound source MAC addresses. The result of the comparison is determined by the setting of "Filter Type."

Required: Yes

Dependencies: "Source MAC Address Mask" on page 6-42 identifies the *significant bits* in the source MAC address defined for this filter.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

Destination MAC Address: This parameter specifies the destination MAC address used in the filter. The filter compares this MAC address against all outbound destination MAC addresses. The result of the comparison is determined by the setting of "Filter Type" on page 6-41.

Required: Yes

Dependencies: "Destination MAC Address Mask" identifies the *significant bits* in the destination MAC address defined for this filter.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

Source MAC Address Mask: This parameter is a *mask* that identifies the significant bits in the source MAC address for the filter. Each bit in the mask corresponds to an identical bit in the source MAC address. For every bit set to one in the mask, the same bit in the MAC address is treated as significant.

When the filter is applied, it compares the significant bits in the source MAC address against the same bits in an outbound source MAC address. Non-significant bits are ignored by the filter. When a mask of all zeros is used, no bits are considered significant; therefore no filtering occurs on outbound source MAC addresses. When a mask of all ones is used (the default), outbound source MAC addresses are compared against the entire source MAC address defined for this filter.

Required: No

Dependencies: None

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: X'FFFF FFFF FFFF'

Destination MAC Address Mask: This parameter is a *mask* that identifies the significant bits in the destination MAC address for the filter. Each bit in the mask corresponds to an identical bit in the destination MAC address. For every bit set to one in the mask, the same bit in the MAC address is treated as significant.

When the filter is applied, it compares the significant bits in the destination MAC address against the same bits in an outbound destination MAC address. Non-significant bits are ignored by the filter. When a mask of all zeros is used, no bits are considered significant; therefore no filtering occurs on outbound destination MAC addresses. When a mask of all ones is used (the default), outbound destination MAC addresses are compared against the entire destination MAC address defined for this filter.

Required: No

Dependencies: None

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: X'FFFF FFFF FFFF'

Outbound Source SAP Filters

A maximum of 128 outbound source SAP filters can be defined on a port.

Status of All Defined Outbound Source SAP Filters on This Port: This parameter enables or disables all outbound source SAP filters defined for a transparent bridge port. When no outbound source SAP filters are defined, the parameter does not affect configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Filter Type: This parameter specifies how the outbound source SAP filters you define are to be interpreted. When this parameter is set to **Permit**, only those frames with the SAP values you specify are bridged over this port. All other frames are rejected. When this parameter is set to **Deny** (the default), all frames **except** those with the SAP values you specify are bridged over this port. Frames containing the SAP values you specify are rejected.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

List of Outbound Source SAP Filters

The following parameter is configured for each outbound source SAP filter that is defined.

Source SAP Value: This parameter specifies the source SAP value used in the filter. The filter compares this SAP value against all outbound source SAP values. The result of the comparison is determined by the setting of "Filter Type."

Required: Yes

Dependencies: None

Valid Values: X'02' to X'FE' in increments of 2

Default Value: None

Outbound Ethernet Type Filters

A maximum of 32 outbound Ethernet Type filters can be defined on a port. This filter is applied to the contents of the Type field within an Ethernet frame. The Type field identifies the type of data encapsulated within an Ethernet Version 2 frame or IEEE 802.3 frame with a SNAP header.

Status of All Defined Outbound Ethernet Type Filters on This Port: This parameter enables or disables all outbound Ethernet Type filters defined for a transparent bridge port. When no outbound Ethernet Type value filters are defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Filter Type: This parameter specifies how the outbound Ethernet Type filters you define are to be interpreted. When this parameter is set to **Permit**, only those frames with the Ethernet Type values you specify are bridged over this port. All other frames are rejected. When this parameter is set to **Deny** (the default), all frames **except** those with the Ethernet Type values you specify are bridged over this port. Frames containing the Ethernet Type values you specify are rejected.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

List of Outbound Ethernet Type Filters

The following parameters are configured for each Ethernet Type filter that is defined.

Ethernet Type: This parameter specifies the Ethernet Type value used in the filter. The filter compares this Ethernet Type value against all outbound Ethernet Type values. The result of the comparison is determined by the setting of "Filter Type."

Required: Yes

Dependencies: None

Valid Values: X'0000' to X'FFFF'

Default Value: None

Ethernet Type Mask: This parameter is a *mask* that identifies the significant bits in the Ethernet Type value for the filter. Each bit in the mask corresponds to an identical bit in the Ethernet Type value. For every bit set to one in the mask, the same bit in the Ethernet Type value is treated as significant.

When the filter is applied, it compares the significant bits in the Ethernet Type value against the same bits in an outbound Ethernet Type value. Non-significant bits are ignored by the filter. When a mask of all zeros is used, no bits are considered significant; therefore no filtering occurs on outbound Ethernet Type values. When a mask of all ones is used (the default), outbound Ethernet Type values are compared against the entire Ethernet Type value defined for this filter.

Required: Yes

Dependencies: None

Valid Values: X'0000' to X'FFFF'

Default Value: X'FFFF'

Outbound Sliding Window Filters

A maximum of 16 outbound sliding window filters can be defined on a port. A sliding window filter enables you to create a filter for any portion of an outbound frame. You define the contents of a *window* area (which is a block of bytes) and an appropriate offset value. The filter compares the window you define against a byte area at the same offset in an outbound frame. The result of this comparison is determined by the setting of "Filter Type" on page 6-37.

Status of All Defined Outbound Sliding Window Filters on This Port: This parameter enables or disables all outbound sliding window filters defined for a transparent bridge port. When no outbound sliding window filters are defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Filter Type: This parameter specifies how the outbound sliding window filters you define are to be interpreted. When this parameter is set to **Permit**, only frames that contain the sliding window bytes you specify are bridged over this port. All other frames are rejected. When this parameter is set to **Deny** (the default), all frames **except** those that contain the sliding window bytes you specify are bridged over this port. Frames that contain the sliding window bytes you specify are rejected.

Required: No

Dependencies: None

Valid Values: Deny, Permit

Default Value: Deny

List of Outbound Sliding Window Filters

The following parameters are configured for each sliding window filter that is defined.

Filter Name: This parameter specifies the name of the sliding window filter.

Required: Yes

Dependencies: None

Valid Values: 1 to 16 characters

Default Value: None

Offset Starting Field: This parameter specifies where the sliding window filter should be applied in an outbound frame. When you select **MAC**, the sliding window filter is applied at an offset calculated from the beginning of the frame. When you select **Data**, the sliding window filter is applied at an offset calculated from the beginning of the Data field in the frame. The size of the offset is determined by the parameter “Offset into Frame” on page 6-46.

Required: No

Dependencies: None

Valid Values: MAC, Data

Default Value: MAC

Offset into Frame: This parameter specifies a byte offset used in calculating where the sliding window filter should be applied in an outbound frame.

Required: No

Dependencies: This parameter and “Offset Starting Field” are used to calculate where the sliding window filter should be applied. “Offset Starting Field” determines the starting point in the frame. The sliding window filter is applied at the offset from this starting point specified by this parameter.

Valid Values: 0 to 1513 bytes

Default Value: 0

Sliding Window Contents: This parameter specifies the contents of the sliding window.

Required: Yes

Dependencies: None

Valid Values: A string of up to 30 hexadecimal bytes. Each byte contains 2 hexadecimal digits (00 to FF). The string must end on a byte boundary.

Default Value: None

Sliding Window Mask: This parameter is a *mask* that identifies the significant bits in the string defined for “Sliding Window Contents.” Each bit in the mask corresponds to an identical bit in the sliding window contents. For every bit set to one in the mask, the same bit in the sliding window contents is treated as significant.

When the filter is applied, it compares the significant bits in the sliding window contents against bits in an outbound frame. The bit comparison begins at an offset into the frame defined by the parameters “Offset Starting Field” and “Offset into Frame.” Non-significant bits are ignored by the filter. When a mask of all zeros is used, no bits are considered significant; therefore no filtering occurs on the outbound frame. When a mask of all ones is used (the default), all bits in the sliding window are compared against bits at the defined offset in the outbound frame.

Required: No

Dependencies: None

Valid Values: A string of up to 30 hexadecimal bytes. Each byte contains 2 hexadecimal digits (00 to FF). Any bytes in the mask beyond what is specified for the sliding window contents are ignored. When the mask contains fewer bytes than the number of bytes specified for the sliding window contents, the missing bytes will be treated as zeros and the corresponding bytes in the sliding window contents will not be treated as significant.

Default Value: A string of 30 hexadecimal bytes, each with a value of X'FF'.

Outbound Filter Order

The parameters in this section enable you to change the order in which outbound transparent bridge filter types are applied on the port being configured. These parameters override the default filter order set by the system configuration parameters for transparent bridging. The default filter order is:

1. Source SAP filters
2. Ethernet Type filters
3. MAC address filters
4. Sliding window filters.

To override the default filter order on a specific port, specify a value for each port filter type parameter. The value indicates the order in which the filter type will be applied to outbound frames. A value of **2**, for example, indicates that the filter type will be applied second. A value must be entered for each available filter type.

Change Order Filters Are Applied on This Port and Override System Settings:

When this parameter is enabled, you can change the order in which outbound filter types are applied on the transparent bridge port being configured. The order you specify overrides the order defined by the system configuration parameters for transparent bridging.

Note: The order you specify affects **only** outbound transparent bridge filter types on the port being configured.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Source SAP Filter: This parameter controls when the outbound source SAP filter type is to be applied on the transparent bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which outbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 4, where 1 specifies that this filter type should be applied **first**, and 4 specifies that this filter type should be applied **last**.

Default Value: None

Ethernet Type Filter: This parameter controls when outbound Ethernet Type filters are to be applied on the transparent bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which outbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 4, where 1 specifies that this filter type should be applied **first**, and 4 specifies that this filter type should be applied **last**.

Default Value: None

MAC Address Filter: This parameter controls when the outbound MAC address filter type is to be applied on the transparent bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which outbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 4, where 1 specifies that this filter type should be applied **first**, and 4 specifies that this filter type should be applied **last**.

Default Value: None

Sliding Window Filter: This parameter controls when the outbound sliding window filter type is to be applied on the transparent bridge port being configured. The order in which filter types are applied on the port is determined by the setting of this parameter in conjunction with the other filter ordering parameters.

Required: See *Dependencies*.

Dependencies: This parameter is required if you choose to change the order in which outbound filter types are applied on a port. The value of this parameter cannot match the value specified for another filter type.

Valid Values: 1 to 4, where 1 specifies that this filter type should be applied **first**, and 4 specifies that this filter type should be applied **last**.

Default Value: None

SNA Port Parameters

Use the worksheet on page A-34.

Enable SNA Frame Forwarding on This Port: This parameter defines whether you want to enable or disable forwarding for SNA frames that contain the values configured for the "SAP Value." When this parameter is set to **Enable**, SNA frames are forwarded on this port.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

List of SAP Values for Frame Forwarding

The following parameters are configured once for each unique SAP value that is used for SNA frame forwarding. SAP value 00 and 04 is included in the list. You can select as many values as you want from the list.

SAP Value: This parameter specifies the service access points (SAPs) that are to be forwarded to the data link switching function by the bridging function.

Required: Yes

Dependencies: None

Valid Values: X'00' to X'EC'

Default Value: None

NetBIOS Port Parameters

Use the worksheet on page A-34.

Data link switching passes the list of service access point values to NetBIOS using source route bridging or transparent bridging. SAP X'F0' is reserved for NetBIOS.

Forward NetBIOS Frames on This Port: This parameter enables or disables the forwarding of NetBIOS traffic on this port.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Forward NetBIOS Datagram and Datagram Broadcast Message on This Port: This parameter enables or disables forwarding NetBIOS datagrams and datagram broadcast messages outbound from other IBM 6611s on this port. This parameter does not affect forwarding inbound NetBIOS datagram and datagram broadcast messages received on this port to other IBM 6611s.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

IP Port Parameters

Use the worksheet on page A-29.

The Internet Protocol (IP) is the protocol that defines an unreliable, connectionless, delivery mechanism for the TCP/IP suite.

IP must be enabled to ensure that you can connect to the IBM 6611 over the IP network for configuration and System Manager functions.

Restrictions: None

Enable IP Routing on This Port: This parameter enables or disables routing of IP packets on this port.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

IP Address: This parameter identifies the IP address of this port.

Required: Yes

Dependencies: The address configured for this port must be unique and cannot be the same address of any other port on the IBM 6611 or in the IP network.

Valid Values: The ranges are defined for the following address classes:

Class A	1.0.0.1 through 127.255.255.254
Class B	128.1.0.1 through 191.255.255.254
Class C	192.0.1.1 through 223.255.255.254

Default Value: None

Subnet Mask: When this parameter is selected, you must enter a subnet mask between 000.000.000.00 to 255.255.255.255 with the appropriate considerations for Class A, B, and C.

Required: No

Dependencies: The subnet mask must cover the network portion of the IP address. This parameter is also required on serial adapter ports using PPP.

Valid Values: The mask ranges are defined for the following address classes:

Class A	255.0.0.0 to 255.255.255.255
Class B	255.255.0.0 to 255.255.255.255
Class C	255.255.255.0 to 255.255.255.255

Default Value: None

Maximum Transmission Unit: The maximum transmission unit (MTU) is the maximum number of bytes per packet of data that will be transmitted from this port. The largest IP packet that can be transmitted is the MTU value. The MTU includes the IP header.

Required: No

Dependencies: None

Valid Values: Table 6-2 show the valid values and default value or this parameter.

Table 6-2. Valid Values and Default Values for Maximum Transmission Unit

Adapter	Valid Values (in bytes)	Default Value (in bytes)
Token-Ring Network 16/4 Adapter (4 MB)	256 to 4472	1492
Token-Ring Network 16/4 Adapter (16 MB)	256 to 17 800	1492
Ethernet (using IEEE Version 2 standards)	256 to 1500	1500
Ethernet (using IEEE 802.3 standards)	256 to 1492	1492
EIA 422/449 Serial Adapter or V.35/V.36 Serial Adapter	256 to 2048	1500
X.25	256 to 1024	576

Default Value: See Table 6-2.

IP Port Filters

The IBM 6611 enables you to specify IP filters at the system level and at the adapter port level on these adapters:

- Ethernet Adapter
- Token-Ring Network 16/4 Adapter
- EIA 422/449 Serial Adapter
- V.35/V.36 Serial Adapter.

IP filters specified at the system level are applied to inbound IP traffic that is received on any 6611 adapter port that is configured for IP and supports IP filters. (See "Packet Filters" on page 3-92 for the system-level IP filter parameters.) IP filters specified at the adapter port level are applied only to inbound IP traffic that is received on that particular port.

IP filters either permit or deny the passing of specific traffic through the IBM 6611. The filters operate in a linear sequence based on the ID number, reflecting the order in which the filtration occurs. For example, if you want to accept only one address from a specific network, you must add a filter with one IP filter ID to permit traffic from the specific network address, and then, add a filter with a higher IP filter ID to deny all other traffic from that network.

A singular filter can be for a specific host address, an entire subnetwork, an entire network, all traffic, or combinations of the three. A singular filter applies to both source and destination addresses. Dual filters apply to a source and destination pair. Dual filters allow traffic to flow or not flow between two specific hosts,

subnetworks, networks, or combinations of the three. To specify the device to be filtered, an address and filter mask must be used. You should understand subnet masking to determine a filter's coverage. Wherever the mask contains a zero, for example 0.0.0.0, all traffic can be permitted or denied. However, for a mask of 255.255.255.255, all address bits are significant, and the filter applies to a single address or host. For example:

IP Address = 9.67.2.2; Filter Mask = 255.0.0.0
Therefore, filters all traffic from network 9.0.0.0

IP Address = 9.67.2.2; Filter Mask = 255.255.0.0
Therefore, filters all traffic from subnetwork 9.67.0.0

IP Address = 9.67.2.2; Filter Mask = 0.0.0.0
Therefore, filters all traffic from all hosts.

Note: These filter masks do not have to line up with the subnet masks used for routing. (For example, you can use a subnet mask of 255.255.0.0 for class A in a network using 9.0.0.0, and you can enter a filter with the IP address of 9.67.2.2 and the filter mask is 255.254.0.0.) This combination would filter out subnets 9.67 and 9.66.

Filters affect the throughput capabilities of the IBM 6611. Therefore, filter arrays must be concise. Dual filters should be added to the end of the list when possible.

Status of All Defined IP Filters On This Port: This parameter enables or disables all IP filters that are specified for a port. If IP port filters are not specified, this parameter does not affect configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

List of IP Port Filters

The following parameters are used when adding an IP filter to a specific adapter port.

IP Filter ID: This parameter specifies the ID of a port-level IP filter (an IP filter that is applied to inbound IP traffic received on a specific 6611 adapter port).

The IP filter ID should be selected according to the sequence in which the incoming traffic is filtered. A filter with a lower ID is enabled before a filter with a higher ID. For example, if you want to permit access to a specific host, but want to deny access to the rest of the network, the permit filter (in this case, the host) must have a lower ID than the deny filter (in this case, the network). Otherwise, the deny removes all traffic from that network, including the host to which you want to permit access.

Notes:

1. An IP filter ID used to specify a system-level filter on the 6611 cannot be used to specify a port-level filter on the same 6611. (See "Packet Filters" on page 3-92 for more information on the system-level IP filter parameters.)
2. An IP filter ID used to specify a port-level filter on one port of the 6611 can be used to specify a port-level filter on another port of the same 6611.

Required: Yes

Dependencies: None

Valid Values: 1 to 50

Default Value: The next unused ID value

Filter Type: This parameter specifies the type of filter for a specific IP filter ID. When this filter is set to **Singular**, it identifies a host, a subnetwork, a network, all hosts, or a combination with a single expression. When this filter is set to **Dual**, the filter identifies two end points from which to deny or allow traffic.

Singular Filters Filter all traffic to and from a specified entity. This is, traffic where the entity is the source that is filtered and traffic where the entity is the destination that is filtered.

Dual Filters Have a direction implied. Meaning that only traffic whose source is a filter address and mask 1, and whose destination is a filter address and mask 2, will be filtered. To limit two entities from communicating with each other through the IBM 6611, two dual filters must be used.

Required: No

Dependencies: None

Valid Values: Singular, Dual

Default Value: Singular

Permit/Deny Traffic: This parameter specifies whether the traffic for a specific IP filter ID is to be permitted through the IBM 6611 or is to be discarded.

Required: No

Dependencies: None

Valid Values: Permit, Deny

Default Value: Permit

Filter IP Address 1: This parameter specifies the address of the host, subnetwork, or network for a specific IP filter ID. For dual filters, this is one of the end points (the source end point). For singular filters, this is the only end point.

Required: Yes

Dependencies: None

Valid Values: A valid IP address

Default Value: None

Filter Subnet Mask 1: This parameter specifies the mask for a specific IP filter ID. The mask, in conjunction with “Filter IP Address 1” on page 6-54, defines the range of IP addresses to be filtered.

Required: No

Dependencies: None

Valid Values: 0.0.0.0 to 255.255.255.255

Default Value: 255.255.255.255

Filter IP Address 2: This parameter specifies the destination address of the host, subnetwork, or network for a specific IP filter ID. This address is used to check the destination field in the packet. This parameter applies only to dual filters. (See “Filter Type” on page 6-54.)

Required: Yes (if the Filter type is specified as **Dual**)

Dependencies: This parameter applies to dual filters only.

Valid Values: A valid IP address

Default Value: None

Filter Subnet Mask 2: This parameter specifies the mask for an IP filter ID. The filter subnet mask, in conjunction with “Filter IP Address 2,” defines the range of IP addresses to be filtered.

Required: No

Dependencies: This parameter applies to dual filters only.

Valid Values: 0.0.0.0 to 255.255.255.255

Default Value: 255.255.255.255

IP Destinations Per DLCI

The following parameters define the DLCI numbers for a list of IP destination addresses.

Destination IP Address: This parameter defines the destination IP address for this DLCI connection on this serial port. The DLCI is configured in “DLCI Number” on page 6-56.

Required: Yes

Dependencies: This parameter is required for each DLCI that is configured.

Valid Values: A valid IP address

Default Value: None

DLCI Number: This parameter is the DLCI number that provides a logical connection to an IBM 6611 with an IP address provided in “Destination IP Address” on page 6-55.

Required: Yes

Dependencies: This parameter is required for each Destination IP Address that is configured.

Valid Values: A valid DLCI

Default Value: None

AppleTalk Port Parameters

Use the worksheet on page A-30.

This section describes the port parameters for configuring the AppleTalk protocol. The IBM 6611 supports AppleTalk Phase 2, which extends the number of AppleTalk nodes that can be associated with a single network and allows nodes within the same network to belong to different AppleTalk zones.

AppleTalk Phase 2 can be defined on the following IBM 6611 adapters:

- Token-Ring Network 16/4 Adapter
- Ethernet Adapter
- EIA 422/449 Serial Adapter (using PPP or Frame Relay)
- V.35/V.36 Serial Adapter (using PPP or Frame Relay).

Network Number Ranges

AppleTalk Phase 2 expands the number of nodes that can be concurrently active on a single AppleTalk network by associating each network with a range of network numbers. Each number in a network's *network number range* can represent up to 253 devices (AppleTalk *nodes*). A network number range of 1–5, for example, can provide addressing for up to 1265 nodes (5 times 253).

AppleTalk Ports

Each AppleTalk port on the IBM 6611 is associated with an AppleTalk network, which is defined on the port. The port is treated as a node on the AppleTalk network and maintains a unique node address within the range of network numbers assigned to the network.

An AppleTalk port is defined as a *seed router port* or *nonseed router port*, depending on the port's role. Nonseed ports acquire network information from a *seed router* attached to the same network. The seed router maintains the configuration data for the network, such as its network number range and zone list. The seed router transmits this information through a seed router port to all other routers directly connected to the network, eliminating the need to separately configure each router port attached to the network. The IBM 6611 can serve as a seed or nonseed router for different AppleTalk networks attached to it.

Network Zone Lists

Each AppleTalk port maintains a *network zone list* for the attached network. Nodes on the network can belong to the zones contained within the network zone list. The list contains the *default zone* for the network and any additional zone names defined by the network administrator when configuring the port.

AppleTalk *zones* provide a way to logically group nodes in an internet regardless of where the nodes are physically located in the internet. Nodes within a zone typically share common characteristics (all nodes in the same department) or provide similar network services (all print servers in the internet). Zones allow users to easily locate and access these nodes.

An AppleTalk node can belong to only one zone. A node's user can assign the node to any one of the zones in the network zone list. Nodes that have not been assigned to a zone belong to the default zone for the network.

AppleTalk Port Filters

As implemented on the IBM 6611, AppleTalk provides two types of port filters:

- Security filters that enable a network administrator to control access to AppleTalk zones and resources in the internet that have been named using special naming conventions. Refer to the AppleTalk description in the *IBM 6611 Network Processor Introduction and Planning Guide* for information about using these filters.
- A network number range filter that provides the capability to filter inbound and outbound AppleTalk packets on each port based on the source and destination network numbers in the packet.

User Restrictions on Routing

The IBM 6611 implementation of AppleTalk also enables a network administrator to select which AppleTalk networks the IBM 6611 will maintain routing information about through a specific port. In addition, the network administrator can select the zones in those networks about which the IBM 6611 will maintain information. This feature restricts the IBM 6611's view of the internet, thereby restricting the view of other routers and non-router nodes that obtain information about the internet from the IBM 6611. This capability is useful for controlling the sharing of sensitive network information with portions of the internet that are under separate administrative control.

For a detailed description of this feature, refer to the *IBM 6611 Network Processor Introduction and Planning Guide*.

Configuration Options

Table 6-3 on page 6-59 summarizes the configuration options for each adapter type that supports the AppleTalk Phase 2 protocol. After configuring AppleTalk on specific ports, you need to enable AppleTalk routing on the IBM 6611 (see "Enable AppleTalk" on page 3-101).

Table 6-3. AppleTalk Configuration Options

WHEN configuring AppleTalk...	THEN optionally...
...on a Token-Ring Network 16/4 Adapter or an Ethernet Adapter: • Enable AppleTalk on the port. • Determine the port type. For seed router ports – Enter the network number range for the network – Enter the default zone name for the network. – Select an initial value for this port's node ID (optional). • Determine whether this port will accept routing information about all networks in the AppleTalk internet or only about selected networks. If you choose to accept information only about selected networks, those networks must be explicitly defined.	• If this is a seed router port, add additional zone names to the network zone list maintained on the port. • Define filters for this port.
...on an EIA 422/449 Serial Adapter or a V.35/V.36 Serial Adapter, using PPP: • Enable AppleTalk on the port. • Determine whether this port will accept routing information about all networks in the AppleTalk internet or only about selected networks. If you choose to accept information only about selected networks, those networks must be explicitly defined. Note: When connecting AppleTalk networks over a point-to-point link, you need to define AppleTalk on the serial adapter ports at each end of the link.	• Define filters for this port.
...on an EIA 422/449 Serial Adapter or a V.35/V.36 Serial Adapter, using Frame Relay: • Enable AppleTalk on the port. • Determine the port type. For seed router ports – Enter the network number range for the network – Enter the default zone name for the network. – Select an initial value for this port's node ID (optional). • Determine whether this port will accept routing information about all networks in the AppleTalk internet or only about selected networks. If you choose to accept information only about selected networks, those networks must be explicitly defined. • Define data link connection identifier (DLCI) numbers for the frame relay connection. Note: When connecting AppleTalk networks over a frame relay connection, you need to define AppleTalk on the serial adapter ports at each end of the connection.	• If this is a seed router port, add additional zone names to the network zone list maintained on the port. • Define filters for this port.

Enable AppleTalk Routing on This Port: This parameter enables or disables the routing of AppleTalk packets on a port. When AppleTalk is disabled, the configuration information defined for the AppleTalk port is retained.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Define Port Characteristics

The following parameters define the characteristics of the AppleTalk port. These parameters do not need to be defined for an EIA 422/449 Serial Adapter or a V.35/V.36 Serial Adapter configured to support PPP.

Port Type: This parameter identifies whether the port is a seed router port or nonseed router port (the default). Nonseed router ports acquire network information from a seed router. The seed router maintains the configuration data for a network, such as its network range and zone list. The seed router transmits this information to all other routers directly connected to the network, eliminating the need to separately configure each router port attached to the network. The IBM 6611 can serve as a seed or nonseed router for different AppleTalk networks attached to it.

Note: When defining a port as a nonseed router port, ensure that the network connected to the port is also connected to at least one seed router port.

Required: No

Dependencies: None

Valid Values: Nonseed router port, Seed router port

Default Value: Nonseed router port

Network Number Range: This parameter specifies the range of network numbers that defines the AppleTalk network attached to the port.

Note: If an AppleTalk network is attached to more than one seed router, the same network number range must be defined on each seed router port.

Required: See *Dependencies*

Dependencies: This parameter is required when this port is a seed router port, as defined by the parameter "Port Type."

Valid Values: A range of consecutive network numbers in the form

lowest network number – highest network number

Each network number can be a value from 1 to 65279. The network numbers are separated by a dash (–). An example of a valid network number range is 98 – 105.

Note: If the range contains a single network number (the lowest and highest numbers in the range are identical), only the one number needs to be entered. The Configuration Program will convert the number you enter (22, for example) into a range (22 – 22).

The network number range specified must be unique within the internet to which this AppleTalk network belongs. The range must not overlap another network number range and network numbers within the range must not be duplicated within the internet.

Default Value: None

Default Zone Name: This parameter specifies the default zone name for the network attached to the port.

The AppleTalk routing function maintains a *zone list* for the AppleTalk network connected to the port. The zone list contains a default zone name and any additional zone names defined for the port (see “Define Additional Zone Names for Network Zone List” on page 6-62). The user of a node can assign the node to one of the zones in the network zone list. Nodes belong to the default zone if they have not been assigned to a specific zone, or if the network zone list contains only the default zone name.

Required: See *Dependencies*

Dependencies: This parameter is required if the port is a seed router port, as defined by the parameter “Port Type” on page 6-60.

Valid Values: A string of 1 to 32 ASCII characters, including blank spaces and special characters. A single asterisk (*) is not allowed as a zone name.

Default Value: None

Starting Value for Node ID Acquisition: This parameter specifies the initial node identifier (*node ID*) used by the AppleTalk port on the IBM 6611 when it attempts to acquire a node address. Each AppleTalk port on the IBM 6611 is treated as a node on the AppleTalk network and maintains a unique node address. The node address consists of a network number (within the range defined for the network) and a node ID. The node address uniquely identifies the node within the AppleTalk internet.

Like other nodes, the AppleTalk port on the IBM 6611 dynamically acquires an internet address each time it is activated. For the network portion of the address, the port selects the first number in the network number range configured for the attached network. For the node ID portion of the address, the port uses the value specified by this parameter. If the resulting address is not in use, it becomes the internet address of the port. If the address is already in use, the port attempts to acquire a new address using the next sequential node ID after the node ID defined for this parameter. This process continues until an available node ID is found. If no available node ID is found for the first network number, the next network number in the range is used.

When the port is stopped and restarted, it will attempt to reuse the last internet address it had acquired. If that address is in use, the port attempts to acquire a new address, starting with the next sequential node ID after the node ID in the previous address.

Required: No

Dependencies: This parameter can be specified if the port is a seed router port, as defined by the parameter “Port Type” on page 6-60.

Valid Values: 1 to 253

Default Value: 1

Define Additional Zone Names for Network Zone List

The following parameter defines additional zone names for the AppleTalk network associated with the port. These zone names are added to the network zone list for the port. The network zone list consists of the default zone name for the network and any additional zones names you define using the following parameter.

A maximum of 254 additional zone names can be defined for the port network.

Additional Zone Name: This parameter defines an additional zone name for the network zone list associated with the port.

Required: No

Dependencies: None

Valid Values: A string of 1 to 32 ASCII characters, including blank spaces and special characters.

A single asterisk (*) is not allowed as a zone name. This character is reserved for use by the AppleTalk protocol.

Default Value: None

Define AppleTalk Filters for the Port

The following parameters define AppleTalk filters for the port being configured. The definition of AppleTalk filters is optional. You can define two types of AppleTalk filters:

- Security filters
- Network number range filters.

Enable Security Filters: This parameter enables or disables the AppleTalk security filters on the port.

The AppleTalk security filters are a set of character filters implemented on the IBM 6611. The filters allow a network administrator to restrict access to particular zones and resources in the AppleTalk internet by using special characters within zone and resource names (# ~ and ~~) When enabled, these filters control responses to zone information and name binding queries coming into the port. The type of filtering performed at the port is based on which special characters are used in the attached network. For a description of the special characters and naming conventions used to restrict access to zone and resource information, refer to the explanation of the AppleTalk protocol in the *IBM 6611 Network Processor Introduction and Planning Guide*.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Enable Network Number Range Filter: This parameter enables or disables the network number range filter defined for the AppleTalk port. The filter compares the source and destination network numbers in inbound and outbound AppleTalk packets against the list of network number ranges defined for the filter. If a source or destination network number falls within one of the network number ranges in the list, the packet is **discarded**. Otherwise, the packet is **forwarded**.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

List of Network Number Ranges

A maximum of 10 network number ranges can be specified for the network number range filter.

Network Number Range: This parameter specifies a range of network numbers used by the network number range filter to evaluate inbound and outbound AppleTalk packets. When the filter is applied, it compares the source and destination network numbers in the packet against the list of network number ranges defined using this parameter. If either the source or destination network number is included in one of the ranges defined, the packet is discarded.

You can filter out all packets received from or destined for a single network number or any range of consecutive network numbers. For example, suppose you want to discard all packets arriving from or destined for network numbers in the range 500 – 600 and network numbers in the range 700 – 800. You could specify each of these ranges for the filter, or specify a single range of 500 – 800 that overlaps the two network number ranges. Note, however, that the range 500 – 800 also filters out any packets from network numbers 601 – 699.

Required: Yes

Dependencies: The parameter “Enable Network Number Range Filter” must be enabled in order to define this parameter.

Valid Values: A range of consecutive network numbers in the form,

lowest network number – highest network number

Each network number can be a value from 1 to 65279. The network numbers are separated by a dash (–). An example of a valid range of network numbers is 98 – 105.

Note: If a single network number is being specified, only that number needs to be entered. The Configuration Program will convert the number you enter (22, for example) into a range (22 – 22).

Default Value: None

Define DLCI Numbers for Frame Relay Connection

The following parameter needs to be specified only when you are defining AppleTalk on an EIA 422/449 Serial Adapter or a V.35/V.36 Serial Adapter configured to support frame relay. The parameter creates a list of DLCIs used to transmit AppleTalk packets.

DLCI Number: This parameter identifies a data link connection identifier (DLCI) that will be used to transmit AppleTalk packets over a frame relay network. Select one of the DLCIs from the list defined for this port.

The frame relay service provider assigns DLCIs for each DTE-to-DTE connection a service requester needs. The IBM 6611 functions as a DTE when defined as part of a frame relay network.

Required: Yes

Dependencies: To specify this parameter, you first need to define the list of DLCIs available on the serial adapter port. See "DLCIs Assigned to This Port" on page 5-20 for more information.

Valid Values: Any of the listed DLCIs

Default Value: None

Restrict Routing to Selected Networks Only

The following parameter enables you to restrict which AppleTalk networks the IBM 6611 maintains routing information about through the port being configured.

Accept Routing Information: This parameter defines whether the port will accept routing and zone information about all networks connected through the port or **only** about selected networks.

When you choose the **ONLY about selected networks** option, you need to define the list of AppleTalk networks that the IBM 6611 will maintain routing and zone information about through the port. (See "List of Selected Networks" on page 6-65.) For networks included in the list, you also can define a list of allowable zone names. The IBM 6611 will ignore information received on the port about networks that are not included in the port's list of selected networks. As a result, the IBM 6611 will not be aware that these networks exist or that routes to these networks are available through the port. Because this option restricts the IBM 6611's view of the internet through this port, it can be used to restrict the view of other routers and non-router nodes that obtain network topology information from the IBM 6611. In this way, a network administrator can restrict the sharing of sensitive network topology or zone information with another portion of the internet that may be under different administrative control.

Required: No

Dependencies: None

Valid Values: About all networks, **ONLY** about selected networks

Default Value: About all networks

List of Selected Networks

The parameters in this section need to be configured when the parameter “Accept Routing Information” on page 6-64 is set to **ONLY about selected networks**. The parameters are used to define each selected network in the list. The IBM 6611 will maintain routing and zone information about each network in the list and will discard routing information received at the port about networks not included in the list.

Network Number Range: This parameter specifies a range of network numbers that identifies an AppleTalk network that the IBM 6611 will accept routing information about through the port.

Required: Yes

Dependencies: None

Valid Values: A range of consecutive network numbers in the form

lowest network number – highest network number

Each network number can be a value from 1 to 65279. The network numbers are separated by a dash (–). An example of a valid network number range is 98 – 105.

Note: If the range contains a single network number (the lowest and highest numbers in the range are identical), only the one number needs to be entered. The Configuration Program will convert the number you enter (22, for example) into a range (22 – 22).

Default Value: None

Filter Traffic to and from Selected Networks

The following parameter is optional and can be configured for each selected network you define.

Enable Network Number Range Filter: This parameter enables or disables a network number range filter that evaluates AppleTalk traffic flowing to and from the selected network. By using this filter, you can control which networks communicate with the selected network over the port. The filter compares the source and destination network numbers in inbound and outbound AppleTalk packets against the list of network number ranges defined for the filter. If a source or destination network number falls within one of the network number ranges in the list, the packet is **discarded**. Otherwise, the packet is **forwarded**.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

List of Network Number Ranges

A maximum of 10 network number ranges can be specified for the network number range filter.

Network Number Range: This parameter specifies a range of network numbers used by the network number range filter to evaluate AppleTalk traffic flowing to and from the selected network. When the filter is applied, it compares the source and destination network numbers in the packet against the list of network number ranges defined using this parameter. If either the source or destination network number is included in one of the ranges defined, the packet is discarded.

You can use the filter to control which networks have access to the selected network through the port and to restrict the flow of packets from the selected network. For example, suppose you want to restrict two network number ranges, 500–600 and 700–800, from communicating with the selected network. By specifying these network number ranges for the filter, all packet traffic between the network numbers specified and the selected network would be discarded. You could also specify a single network number range of 500–800 that overlaps the two network number ranges. Note, however, that the range 500–800 also filters out any packet traffic between the selected network and network numbers 601–699.

Required: Yes

Dependencies: The parameter “Enable Network Number Range Filter” on page 6-65 must be enabled for the selected network in order to define this parameter.

Valid Values: A range of consecutive network numbers in the form

lowest network number – highest network number

Each network number can be a value from 1 to 65279. The network numbers are separated by a dash (–). An example of a valid network number range is 98–105.

Note: If a single network number is being specified, only that number needs to be entered. The Configuration Program will convert the number you enter (22, for example) into a range (22–22),

Default Value: None

Define Allowable Zones for Selected Networks

A maximum of 255 zone names can be defined for each selected network. At least one zone name needs to be defined to enable communication with the selected network.

Allowable Zone Name: This parameter defines the name of a zone associated with the selected network. If a zone name appears in the list of zone names defined by this parameter, the port will forward information about the zone to other AppleTalk networks. The port discards information received from the selected network about zones not included in the list.

This parameter can reduce the amount of zone information that is forwarded to other portions of the AppleTalk internet from the selected network. In addition, this parameter can be used to limit access to zone information on the selected network.

Required: Yes

Dependencies: None

Valid Values: A string of 1 to 32 ASCII characters, including blank spaces and special characters.

Default Value: None

IPX Protocol Port Parameters

Use the worksheet on page A-31.

Enable IPX routing on this port: This parameter enables or disables IPX routing on this port. When IPX routing is disabled, the configuration information for IPX on this port is retained.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

IPX Network Number: This parameter assigns an IPX network number to the physical network attached to this port.

An IPX address is a 32-bit, hexadecimal number, followed by a 48-bit MAC address that is also in hexadecimal form. For example:

.000000e7.0020.d0e0.22fd

This example identifies the host name as X'0020.d0e0.22fd', which is located on the network identified as X'000000e7'.

Required: Yes

Dependencies: This parameter is required when "Enable IPX routing on this port" is set to **Enable**.

This parameter is configured for each Token-Ring Network 16/4 Adapter, Ethernet Adapter, or serial adapter port routing IPX packets.

Valid Values: X'0000 0000' to X'FFFF FFFF'

Default Value: None

Encapsulation Method: This parameter determines the logical link control (LLC) encapsulation method used to transmit IPX packets on a Token-Ring Network 16/4 Adapter port.

Required: No

Dependencies: This parameter is configured only when this is a token-ring port.

Valid Values: Token-Ring 802.5, Token-Ring SNAP

Default Value: Token-Ring 802.5

Encapsulation Method: This parameter determines the logical link control (LLC) encapsulation method used to transmit IPX packets on an Ethernet Adapter port.

Required: No

Dependencies: This parameter is configured only when this is an Ethernet port.

Valid Values: Ethernet II, Ethernet SNAP, Ethernet 802.3, Ethernet 802.2

Default Value: Ethernet II

Software Loopback Active: This parameter controls whether packets addressed to the local host will be looped back by the IPX software or the media hardware.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

IPX Destinations Per DLCI

The following parameters are configured to create a list of DLCI numbers to IPX destinations.

Destination IPX Address: This parameter is the destination IPX address for this DLCI connection on a Serial Adapter port. The DLCI number is configured in "Destination IPX Address."

Required: No

Dependencies: None

Valid Values: A MAC address

Default Value: None

DLCI: This parameter is the DLCI number that provides a logical connection to a router with an IPX address provided in the parameter above.

Required: Yes

Dependencies: This parameter is required for each DLCI number configured.

Valid Values: The values configured in "DLCIs Assigned to This Port" on page 5-20.

Default Value: None

IPX Port Filters

These parameters configure IPX port filters. The filtered values are located in the integrated data processing (IDP) header.

Status of All Defined IPX Filters on This Port: This parameter enables or disables all IPX filters defined on this port. When IPX filters are not defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Filtering Mode: This parameter determines the filtering mode for all IPX filters defined on this port. When this port is using deny mode, all IPX packets matching a defined filter are discarded. When this port is using permit mode, all IPX packets are discarded except the packets matching a defined filter.

Required: No

Dependencies: This parameter is configured once for all IPX port filters defined.

Valid Values: Permit, Deny

Default Value: Deny

List of IPX Port Filters

Filter ID: This parameter uniquely defines this filter in a list of filters.

Required: Yes

Dependencies: This parameter is required to define IPX port filters. It is configured once for each filter.

Valid Values: 1 to 10

Default Value: None

Filter on Packet Type: This parameter allow IPX packets to be filtered based on the packet type.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Packet Type Value: This parameter defines the packet type value used to filter IPX packets.

Required: This parameter is required to define IPX port filters.

Dependencies: This parameter is required when "Filter on Packet Type" is set to **Enable**.

Valid Values: X'00' to X'FF'

Default Value: None

Transport Control Attributes

Filter on Transport Control: This parameter allows IPX packets to be filtered based on transport control (hop count).

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Transport Control Value: This parameter defines the transport control value used to filter IPX packets.

Required: No

Dependencies: This parameter is required when “Filter on Transport Control” is required.

Valid Values: X'0' to X'F'

Default Value: None

Relational Compare Operator: This parameter is used as the relational operator when filtering is based on transport control.

Required: No

Dependencies: This parameter requires “Filter on Transport Control” to be set to **Enable**.

Valid Values:

- Equals
- Less than
- Less than or equal
- Greater than
- Greater than or equal.

Default Value: Equals

Destination Attributes

Filter Based on Destination Network: This parameter allows IPX packets to be filtered based on the destination network value.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Destination Network Value: This parameter defines the destination network value used to filter IPX packets.

Required: Yes

Dependencies: This parameter is required when “Filter Based on Destination Network” is set to **Enable**.

Valid Values: X'0000 0000' to X'FFFF FFFF'

Default Value: None

Filter on Destination Host: This parameter allows a filter on the destination host.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Destination Host Value: This parameter defines the destination host value used to filter IPX packets.

Required: No

Dependencies: This parameter requires “Filter on Destination Host” to be set to **Enable**.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFF'

Default Value: None

Filter on Destination Socket: This parameter allows IPX packets to be filtered on the destination socket.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Destination Socket Value: This parameter defines the destination socket value for IPX destination socket filters.

Required: No

Dependencies: This parameter is required when “Filter on Destination Socket” is set to **Enable**.

Valid Values: X'0000' to X'FFFF'

Default Value: None

Source Attributes

Filter on Source Network: This parameter allows IPX packets to be filtered on the source network.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Source Network Value: This parameter defines the source network value used to filter IPX packets.

Required: No

Dependencies: This parameter is required when “Filter on Source Network” is set to **Enable**.

Valid Values: X'0000 0000' to X'FFFF FFFF'

Default Value: None

Filter on Source Host: This parameter allows IPX packets to be filtered on the source host.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Source Host Value: This parameter defines the source host value used to filter IPX packets.

Required: No

Dependencies: This parameter is required when “Filter on Source Host” is set to **Enable**.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

Filter on Source Socket: This parameter allows IPX packets to be filtered based on the source socket.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Source Socket Value: This parameter defines the source socket value for IPX source socket packet filters.

Required: No

Dependencies: This parameter is configured once for each filter. This parameter requires “Filter on Source Socket” on page 6-73 to be set to **Enable**.

Valid Values: X'0000' to X'FFFF'

Default Value: None

XNS Port Parameters

Use the worksheet on page A-32.

The XNS port parameters are configured to route XNS packets on the following IBM 6611 adapters:

- Token-Ring Network 16/4 Adapter
- Ethernet Adapter
- EIA 422/449 Serial Adapter
- V.35/V.36 Serial Adapter.

Note: The XNS host address is automatically set to the value of the MAC address of the Token-Ring Network 16/4 Adapter and Ethernet Adapter on this port.

Enable XNS Routing on This Port: This parameter enables or disables routing of XNS packets on this port. When XNS routing is disabled, the configuration information for XNS on this port is retained.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

XNS Network Number: This parameter assigns an XNS network number to the physical network attached to this port.

Required: Yes

Valid Values: X'0000 0000' to X'FFFF FFFF'

Default Value: None

Dependencies: None

Encapsulation Method: This parameter determines the LLC encapsulation method used to transmit XNS packets on this Token-Ring Network 16/4 Adapter port.

Required: No

Dependencies: This parameter is configured only for a Token-Ring Network 16/4 Adapter port.

Valid Values: Token-Ring 802.5, Token-Ring SNAP

Default Value: Token-Ring 802.5

Destination Host Address: This parameter is the destination host address of the XNS host at the other end of the link attached to this serial port.

Required: Yes

Dependencies: This parameter is required when a Serial Adapter port is configured for PPP and "Enable XNS Routing on This Port" is set to **Enable**.

Valid Values: X'0000 0000 0001' to X'FFFF FFFF FFFE'

Default Value: None

Encapsulation Method: This parameter determines the LLC encapsulation method used to transmit XNS packets on this Ethernet Adapter port.

Required: No

Dependencies: This parameter is configured only for an Ethernet Adapter port.

Valid Values: Ethernet II, Ethernet SNAP, Ethernet 802.3

Default Value: Ethernet II

Number of Bytes Returned in an Error Protocol Packet: This parameter determines the number of bytes of the original XNS packet returned in an XNS Error protocol packet.

Required: No

Dependencies: None

Valid Values: 42 to 542 bytes

Default Value: 42 bytes

Error Protocol Active: This parameter determines whether XNS Error protocol packets are generated in response to XNS packets that are not valid.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Software Loopback Active: This parameter controls whether XNS packets addressed to the local host are looped back by the XNS software or the media hardware.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

XNS Destinations Per DLCI

The following parameters are configured to create a list of DLCI numbers to XNS destinations.

Destination XNS Address: This parameter defines the destination XNS address for this DLCI connection on a Serial Adapter port. The DLCI number is configured in "DLCI" on page 6-77.

Required: No

Dependencies: None

Valid Values: A MAC address

Default Value: None

DLCI: This parameter is the DLCI number that provides a logical connection to a IBM 6611 with an XNS address that is provided in “Destination XNS Address” on page 6-76.

Required: Yes

Dependencies: This parameter is required to configured each DLCI number

Valid Values: The values configured in “DLCIs Assigned to This Port” on page 5-20.

Default Value: None

XNS Port Filters

A maximum of 128 filters can be defined. These parameters are not required.

Status of All Defined XNS Filters on This Port: This parameter enables or disables all XNS filters defined on this port. When XNS filters are not defined, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

Filtering Mode: This parameter determines the filtering mode for all filters defined on this port. When **Deny** is selected, all packets matching a configured filter are discarded. When **Permit** is selected, all packets are discarded except for the packets matching a configured filter.

Required: No

Dependencies: This parameter is configured once for all XNS port filters.

Valid Values: Permit, Deny

Default Value: Deny

List of XNS Port Filters

Filter ID: This parameter uniquely defines an XNS filter.

Required: Yes

Dependencies: This parameter is required to define XNS port filters.

Valid Values: 1 to 10

Default Value: None

Filter Based on Checksum: This parameter allows XNS packets to be filtered based on the checksum.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Checksum Value: This parameter defines the checksum value used to filter XNS packets.

Required: No

Dependencies: This parameter is required when “Filter Based on Checksum” is enabled.

Valid Values: X'0000' to X'FFFF'

Default Value: None

Filter on Packet Type: This parameter allows XNS packets to be filtered based on the XNS packet type.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Packet Type Value: This parameter defines the XNS packet type value used to filter XNS packets.

Required: No

Dependencies: This parameter is required when “Filter on Packet Type” is set to **Enable**.

Valid Values: X'00' to X'FF'

Default Value: None

Transport Control Attributes

Filter on Transport Control: This parameter allows XNS packets to be filtered based on transport control (hop count).

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Transport Control Value: This parameter defines the transport control value used to filter XNS packets.

Required: No

Dependencies: This parameter is required when “Filter on Transport Control” on page 6-78 is set to **Enable**.

Valid Values: X'0' to X'F'

Default Value: None

Relational Compare Operator: This parameter is used as the relational operator when filtering is based on transport control.

Required: No

Dependencies: This parameter is required when “Filter on Transport Control” on page 6-78 is set to **Enable**.

Valid Values:

- Equals
- Less than
- Less than or equal
- Greater than
- Greater than or equal.

Default Value: Equals

Destination Attributes

Filter Based on Destination Network: This parameter allows XNS packets to be filtered based on the XNS destination network number.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Destination Network Value: This parameter defines the Destination Network Value used to filter XNS packets.

Required: No

Dependencies: This parameter is required when “Filter Based on Destination Network” is set to **Enable**.

Valid Values: X'0000 0000' to X'FFFF FFFF'

Default Value: None

Filter on Destination Host: This parameter allows a filter on the destination host.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Destination Host Value: This parameter defines the destination network value used to filter XNS packets.

Required: No

Dependencies: This parameter is required when “Filter on Destination Host” on page 6-79 is set to **Enable**.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

Filter on Destination Socket: This parameter allows XNS packets to be filtered on the destination socket for XNS destination socket filters.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Destination Socket Value: This parameter defines the destination socket value for XNS destination socket filters.

Required: No

Dependencies: This parameter is required when “Filter on Destination Socket” is set to **Enabled**.

Valid Values: X'0000' to X'FFFF'

Default Value: None

Source Attributes

Filter on Source Network: This parameter allows XNS packets to be filtered on the source network.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Source Network Value: This parameter defines the source network value used to filter XNS packets.

Required: No

Dependencies: This parameter is required when “Filter on Source Network” is enabled.

Valid Values: X'0000 0000' to X'FFFF FFFF'

Default Value: None

Filter on Source Host: This parameter allows XNS packets to be filtered on the source host.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Source Host Value: This parameter defines the source host value used to filter XNS packets.

Required: No

Dependencies: This parameter is required when “Source Host Value” is set to **Enable**.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: None

Filter on Source Socket: This parameter allows XNS packets to be filtered based on the source socket.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Disable

Source Socket Value: This parameter defines the source socket value for XNS source socket packet filters.

Required: No

Dependencies: This parameter is required when “Filter on Source Socket” is set to **Enable**.

Valid Values: X'0000' to X'FFFF'

Default Value: None

DECnet Port Parameters

Use the worksheet on page A-33.

These parameters configure DECnet on a port of the IBM 6611.

Enable DECnet on This Interface: The parameter allows you to enable or disable the DECnet protocol on this port.

Required: Yes

Dependencies: This parameter is required to forward DECnet packets.

Valid Values: Enable, Disable

Default Value: Disable

Remote DECnet Address: This parameter contains the DECnet address of the IBM 6611 at the other end of the serial link attached to this frame relay port.

Required: Yes

Dependencies: None

Valid Values: <A DECnet area number> . <A DECnet node number>

Default Value: None

Remote DECnet Node Type: This parameter provides a default value of the node connected to the other end of the serial link.

Required: No

Dependencies: None

Valid Values: Area, Routing-IV, Endnode

Default Value: Area

Circuit Cost: This parameter determines the cost of using the circuit. A higher cost reduces traffic on the circuit because the routing layer forwards packets on the least costly path to a destination. Before you set this parameter, you should check the values of "Maximum Cost" on page 3-117 and "Area Maximum Cost" on page 3-117 to be sure they are greater than or equal to the total circuit cost for nodes or areas which are at the maximum distance.

Required: No

Dependencies: All hosts on the same segment must share the same value.

Valid Values: 1 to 63

Default Value: None

Hello Timer: This parameter specifies how often the IBM 6611 sends Hello messages. The IBM 6611 broadcasts Hello messages on all circuits. Other hosts on the network use the Hello messages to identify the hosts with which they can communicate directly.

Required: No

Dependencies: None

Valid Values: 1 to 8191 seconds

Default Value: 15 seconds

Router Priority: This parameter sets the priority that this IBM 6611 is to have in selecting a designated router on the attached LAN segment. The DECnet protocol selects the router with the highest priority value as the default router. When several routers have the same priority, the protocol selects the one with the highest address.

Required: No

Dependencies: None

Valid Values: 0 to 127

Default Value: 64

Routing Timer: Routing messages are sent automatically when changes in the network occur. They also are sent at intervals to ensure that all routing nodes have up-to-date information. This interval is determined by this parameter. This time is referred to as a routing time for non-broadcast circuits and a broadcast routing time for broadcast circuits. When the routing timer for a circuit expires, routing messages are sent on that circuit.

Required: No

Dependencies: None

Valid Values: 1 to 65535 seconds

Default Value: 40 seconds (broadcast circuits); 600 seconds (non-broadcast circuits)

Maximum Routers: This parameter defines the maximum number of routers that are allowed on a specific circuit. This parameter helps you set the maximum number of routers for each circuit.

Required: No

Dependencies: None

Valid Values: 1 to 1022

Default Value: 32

List of DLCI Numbers to DECnet Destinations

DLCI Number: This parameter is the DLCI number that is used to communicate with the destination defined in "Remote DECnet Address" on page 6-84 and "Remote DECnet Node Type" on page 6-84.

Required: Yes

Dependencies: None

Valid Values: A valid DLCI number

Default Value: None

Remote DECnet Address: This parameter contains the DECnet address of the IBM 6611 at the other end of the serial link attached to this frame relay port.

Required: Yes

Dependencies: This parameter is required when “Use Inverse ARP to Resolve Remote Protocol Addresses” on page 5-20 is set to **Disable**.

Valid Values: <A DECnet area number> . <A DECnet node number>

Default Value: None

Remote DECnet Node Type: This parameter defines a default value of the node connected at the other end of the serial link.

Required: No

Dependencies: None

Valid Values: Area, Routing-IV, Endnode

Default Value: Area

DECnet Port Filters

“Filter ID” and “Direction in Which the Packet Is Moving” are configured for each packet filter configured for a DECnet port. Configuring DECnet packet filter parameters is not required.

Status of All Defined DECnet Filters on This Port: This parameter enables or disables all DECnet filters defined for this port. When DECnet filters are not defined for this port, this parameter does not affect the configuration.

Required: No

Dependencies: None

Valid Values: Enable, Disable

Default Value: Enable

List of Packet Filters

Filter ID: This parameter identifies which filter will be applied on this port.

Required: No

Dependencies: This parameter is required to define DECnet packet filters.

Valid Values: Any filter ID entered in the list of packet filters configured in the DECnet parameters starting on page 3-120 and ending on page 3-121.

Default Value: None

Direction in Which the Packet Is Moving: This parameter identifies the direction in which a DECnet packet must be moving to apply this filter.

Required: No

Dependencies: None

Valid Values: Inbound, Outbound, Inbound and Outbound

Default Value: Inbound and Outbound

Part II: Using the System Manager

The chapters in “Part II: Using the System Manager” are:

Chapter 7. Operating the System Manager	7-1
Chapter 8. Using the Fast-Path Environment and Command Primitives	8-1
Chapter 9. Accessing the IBM 6611	9-1
Chapter 10. Operating the IBM 6611	10-1
Chapter 11. Problem Determination	11-1
Chapter 12. Using the Software Installation and Maintenance Facility	12-1
Chapter 13. Using Concurrent Diagnostics and Hardware Vital Product Data	13-1
Chapter 14. Using the System Manager to Configure the IBM 6611	14-1

Chapter 7. Operating the System Manager

Introduction to System Manager	7-2
Using the System Manager Screens	7-3
Menu Screens	7-4
Selector Screens	7-6
Dialog Screens	7-7
Command Status Screens	7-9
Using the Function Keys in the System Manager	7-11
Making Selections from a List of Choices	7-13
Getting System Manager Help	7-14
Contextual Help	7-14
General Help	7-14
Performing System Manager Tasks	7-16
Flowchart of System Manager Menu Screens	7-17
Performance and Statistics	7-22
Problem Determination Facilities	7-23
Concurrent Hardware Diagnostics	7-25
Resource Control and Management	7-27
System Environment and Configuration	7-28
Remote Accesses to Other Nodes	7-30
Software Installation and Maintenance	7-31
Hardware Vital Product Data	7-34
Configuration Files and Reports	7-35
Adapter and Protocol Configuration	7-36

Introduction to System Manager

The IBM Multiprotocol Network Program System Manager (*System Manager*) is a menu-driven user interface that is designed to simplify system management and operation tasks. The System Manager supports tasks for performing change management, network management, and problem determination, and many system operations. It is invoked automatically whenever the IBM 6611 is accessed through the S1 or S2 serial ports or by using the **telnet** or **rlogin** commands. For more information about accessing the IBM 6611, see Chapter 9.

Using the System Manager Screens

The System Manager has these four major types of screens:

- Menu screens
- Selector screens
- Dialog screens
- Command status screens.

Other supporting screens in the System Manager include:

Contextual help screens

Describe specific help information for a given field. On menu screens, the help information describes the task that the menu item performs. On dialog screens, the help information gives instructions for data entry in a field. On selector screens, the help information describes the list of items to select.

General help screens

Contain help information either for the entire System Manager or for a specific screen type. General help for the entire System Manager is invoked from the System Manager main menu, and from within each contextual help screen, information message screen, and error message screen. General help for screen types is available on pop-up list screens, field edit screens, and command status screens.

Information message screens

Give status information when attempting to execute a task.

Error message screens

Identify problems that occur when attempting to execute a task.

Pop-up list screens

Appear when F4 (Esc + 4) is pressed on an entry field of a dialog screen that contains a list of options that can be selected for the given dialog item. These dialog items contain a “+” on the right side of the screen.

Field edit screens

Appear when F6 (Esc + 6) is pressed on a field of a dialog screen that can be edited.

Menu Screens

Figure 7-1 shows the main menu screen of the System Manager.

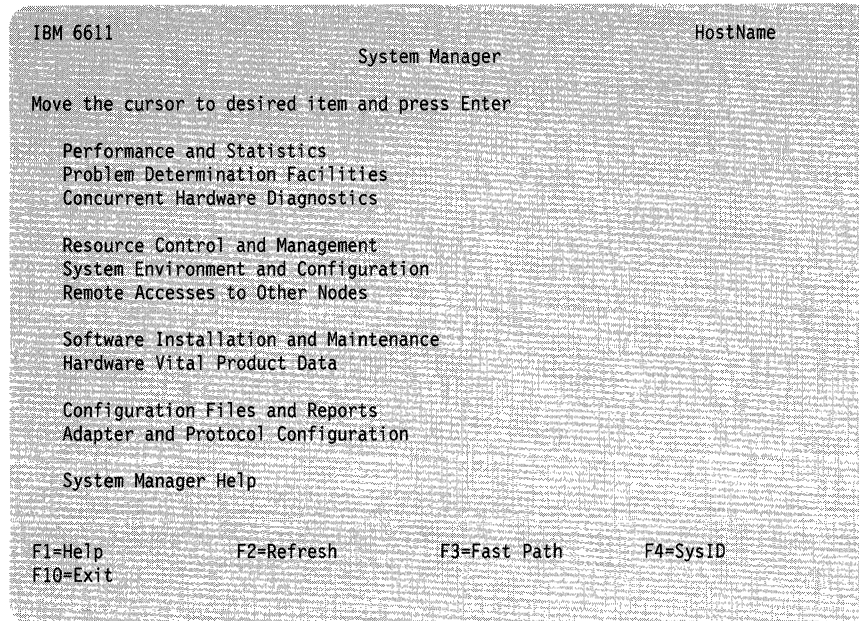


Figure 7-1. System Manager Main Menu

Each menu screen has a list of items that can be selected to perform a specific task or group of tasks that are described by the menu item. In the top right corner of the menu screen, the host name that is associated with this IBM 6611 appears, if configured. The host name is only updated when the user logs in. If the host name changes during the log in session and you want the new name to appear on the screen, you need to exit the IBM 6611 and log in again. The menu title appears on the second line of the menu screen. The function keys appear at the bottom of the menu screen. The list of menu items appear on the left side of the screen.

To select a menu item, use the up and down arrow keys to move the cursor beside the menu item. With many terminal types, the selected menu item is shown in reverse video. Press **Enter** to select the menu item. One of the following screens appears:

- Another menu screen
- A command status screen
- A selector screen
- A dialog screen.

Contextual help is available for each menu item. To get help for a menu item, position the cursor beside the menu item you want and press **F1 (Esc + 1)**.

From each of the menu screens, you can quickly reference some high-level system configuration information. Press **F4 (Esc + 4)**, labeled SysID, to view this information. Please refer to Figure 7-2 on page 7-6 for the System Manager panel. This information can be viewed only when it is configured. The configuration information includes:

- Host name

The host name must be configured using either the Configuration Program ("IBM 6611 Host Name" on page 4-3) or the System Manager ("Setting Host Name Information" on page 10-35).

- Model number

The model number is added to the hardware vital product data during the manufacturing process. If you replace your hard disk, it may be necessary to update the hardware vital product data with the model number.

You can configure the serial number using the fast path command:
hw_serial_model.

- Serial number

The serial number is added to the hardware vital product data during the manufacturing process. If you replace your hard disk, it may be necessary to update the hardware vital product data with the serial number.

You can configure the serial number using the fast path command:
hw_serial_model.

- Configuration name

The configuration name is the name of the configuration currently running in the IBM 6611. If the current configuration was sent from the Configuration Program, the name is the one that was specified when you saved the configuration. If the current configuration was updated last with the System Manager, the name has the format: localhost(userid) Date Time. The *userid* is the user name that was used to update the current configuration at the date and time specified. Any configuration change made from the System Manager must be **applied** or **committed** for it to become the current configuration.

- Configuration status.

The configuration status presented is from the perspective of the user who has pressed **F4 (Esc + 4) = SysID** to view this information. The configuration status is:

current: all configuration changes made from the userid that you are logged into have been committed. However, there may be unapplied or applied configuration changes made from a different userid. If another user has some applied, but not committed changes, the configuration name will have the localhost format. The userid will contain the name of the user who has applied, but not committed the last configuration changes. The only way to determine if there are unapplied configuration changes is to login with each controlling userid and press **F4 (Esc + 4) = SysID** to view its configuration status.

applied: the userid that you are logged into has some applied, but not committed configuration changes.

unapplied: the userid that you are logged into has some unapplied configuration changes. These changes are unnamed. Thus the configuration name is not associated with these changes.

partially applied: the userid that you are logged into has some applied and unapplied configuration changes.

When viewing the System Configuration Information screen, press **Enter** to return to the System Manager menu screen.

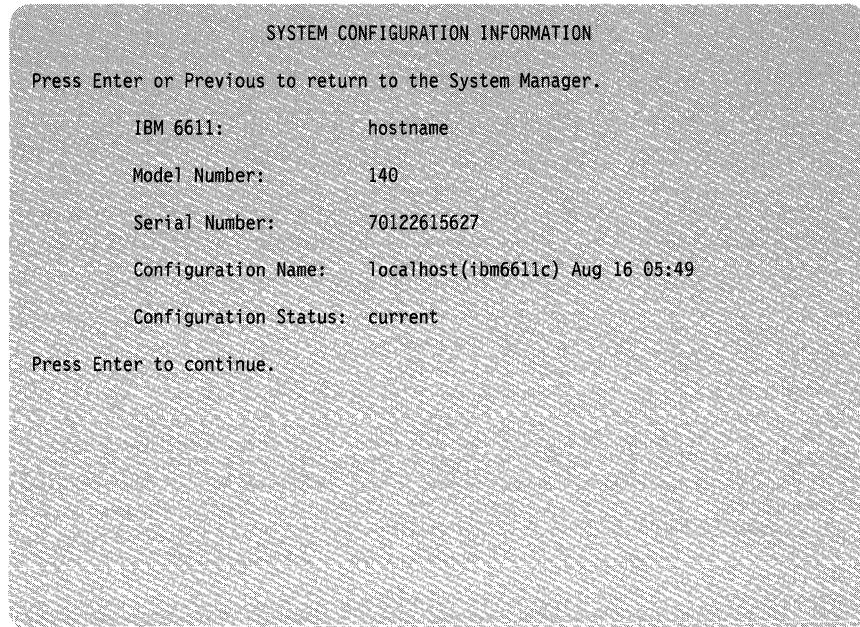


Figure 7-2. System Configuration Information Screen

Selector Screens

Figure 7-3 is an example of a selector screen in the System Manager.

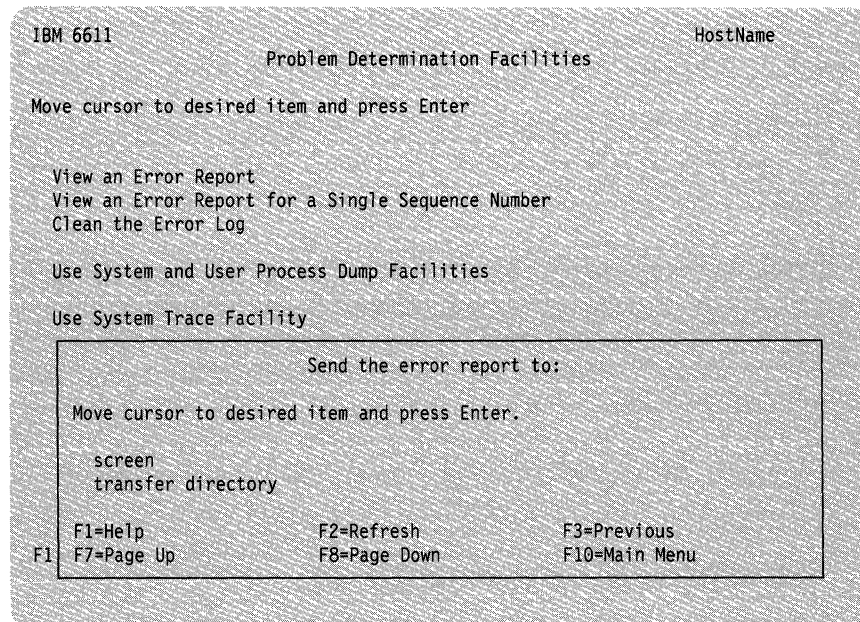


Figure 7-3. Example of a Selector Screen

A selector screen displays a list of options from which a selection must be made to complete the task. This screen appears between menu screens and dialog or command status screens throughout the System Manager. The type of item to be selected appears at the top of the screen. The function keys appear at the bottom of the screen. The selection list appears on the left side of the screen.

To select an option on a selector screen, use the up and down arrow keys to place the cursor beside the item in the selection list. When the list cannot be displayed on one screen, use the arrow keys to scroll through the list. You can also use the PageUp and PageDown function keys or key sequences to scroll. For more information about function keys and key sequences, see Table 7-1 on page 7-11.

For lists that are too long to be displayed on one screen, the following indications appear at the top or bottom of the list.

[TOP] Indicates the top of the list

[BOTTOM] Indicates the bottom of the list

[MORE...nn] Indicates that *nn* items of the list are not displayed on the screen.

Place the cursor on the item to be selected and press **Enter** to select the item. One of the following screens appears:

- Another selector screen
- A command status screen
- A dialog screen.

Contextual help is available for the group of selection items. To get help, press **F1 (Esc + 1)** from any position on the screen.

Dialog Screens

Figure 7-4 is an example of a dialog screen in the System Manager.

View an Error Report

Type or select values in entry fields.
Press Enter after making all desired changes.

Style of error report	[Entry Fields]	
Error classes (default is all)	summary	+
Error types (default is all)	[]	+
Resource classes (default is all)	[]	+
Resource names (default is all)	[]	+
Error ids to include (default is all)	[]	+X
Error ids to exclude (default is none)	[]	+X
Starting date and time (MMDDhhmmYY)	[]	
Ending date and time (MMDDhhmmYY)	[]	
Destination of error report	screen	

F1=Help F2=Refresh F3=Previous F4=List
F5=Undo F6=Edit F7=Page Up F8=Page Down
F10=Main Menu

Figure 7-4. Example of a Dialog Screen

In a dialog, you provide details about the task you selected. Values are placed into the entry fields on the dialog screen by selecting an item from an option ring, from a pop-up list, or by typing in the value for dialog items that do not have a list. The title of the dialog appears at the top of the screen. The function keys appear at the bottom of the screen. Descriptions of the fields appear at the left side of the screen. Entry fields appear at the right side of the screen.

To select a dialog item, use the up and down arrow keys to move the cursor to the entry field.

The following symbols indicate the various types of entry fields on the dialog screens:

Symbol	Meaning
[]	Indicates an entry field
< >	Indicates more text to the left or right of the visible entry field. Use the right and left arrow keys to scroll the field.

The following symbols appear at the left side of the screen:

Symbol	Meaning
*	Indicates that this dialog item requires a value.

The following symbols appear at the right side of the screen:

Symbol	Meaning
+	Indicates that a list of choices or an option ring is available. A <i>list of choices</i> provides a pop-up list with the selections available for a particular entry field. An <i>option ring</i> allows you to tab through each selection available for a particular entry field. Press F4 (Esc + 4) to display the list of choices. Use the up and down arrow keys to place the cursor on a option in the list that you want to select. Press Enter to select the option for a single selection list. Press F9 (Esc + 9) to select items for a multiple selection list and press Enter to indicate all choices that are selected. When an option ring is available, the entry field is not enclosed in brackets in most instances. Press Tab to display and make a selection from the option ring.
#	Indicates that a numeric value must be supplied.
X	Indicates that a hexadecimal value must be supplied.

When the list of dialog items cannot be displayed on one screen, use the arrow keys to scroll through the items. You can also use the PageUp or PageDown function keys or key sequences to scroll. For more information about function keys or key sequences, see Table 7-1 on page 7-11.

For dialog screens that are too long to be displayed on one screen, the following indications appear at the top or bottom of the list of dialog items.

[TOP]	Indicates the top of the list of dialog items.
[BOTTOM]	Indicates the bottom of the list of dialog items.
[MORE...nn]	Indicates that <i>nn</i> dialog items are not displayed on the screen.

Contextual help is available for each entry field on the dialog screen. To get contextual help, position the cursor on the entry field and press **F1 (Esc + 1)**.

Command Status Screens

Figure 7-5 is an example of a command status screen in the System Manager.

```
COMMAND STATUS

Function name: Protocol Statistics
Command: OK          stdout: yes          stderr: no

Before command completion, additional instructions may appear below.

[TOP]
ip:
    ocIpForwarding = 1
    ocIpDefaultTTL = 255
    ocIpInReceives = 87
    ocIpInHdrErrors = 0
    ocips_toosmall = 0
    ocips_badver = 0
    ocips_badhlen = 0
    ocips_badsum = 0
    ocips_badlen = 0
    ocips_tooshort = 0
    ocips_badttl = 0
[MORE...27]

F1=Help      F2=Refresh      F3=Previous      F7=Page Up
F8=Page Down F10=Main Menu
```

Figure 7-5. Example of a Command Status Screen

The command associated with a selected task is invoked when Enter is pressed on a dialog screen, a selector screen, or a menu screen that does not lead to a dialog screen. A command status screen is displayed as a result of issuing most commands. While the command is executing, the *Command: running* message is displayed in the upper left side of the screen. The function key designations are not displayed. As the output is formatted for the screen a *Processing data ...* message is displayed at the bottom the screen. When the command completes, the *Command: OK* message or *Command: failed* message is displayed in the upper left side of the screen. The first screen of the output is displayed on the screen and the function key designations appear at the bottom of the screen.

When the output cannot be displayed on one screen, use the arrow keys to scroll through the output. You can also use the PageUp or PageDown key sequences to scroll. For more information about function keys or key sequences, see Table 7-1 on page 7-11.

[TOP] Indicates the top of the list

[BOTTOM] Indicates the bottom of the list

[MORE...nn] Indicates that *nn* items of the list are not displayed on the screen.

With some commands, the command status screen is not used for output. The System Manager clears the screen and gives control of the screen to the command being invoked. When the command finishes, control is returned to the System Manager. This is used mainly in situations requiring interactive dialog between you and the command being issued. An example of this scenario is changing passwords.

There are also situations when the System Manager gives control of the screen to the command being invoked and then exits. When the command is completed, System Manager does not regain control of the screen. Therefore, you will have to log in again to the IBM 6611 to restart System Manager.

General help is available for the task output generated on a command status screen. To get general help, press **F1 (Esc + 1)** while viewing the command output.

Using the Function Keys in the System Manager

In the System Manager, function key designations appear at the bottom of the screens. Only the function keys that are valid for the specific screen type are displayed. Table 7-1 describes these function keys.

The key sequences function according to the way the first key functions. All keys are designated by a plus sign (+) separating the keys.

- If the first key is the Esc key, it is pressed and released. The second key is pressed shortly after the Esc key.
- If the first key is a Ctrl or Shift key, it is pressed and held down while the second key is pressed.

Note: The following functions are valid only when your keyboard has not been remapped.

Table 7-1 (Page 1 of 2). System Manager Function Keys

Function Key	Meaning	Description
F1 or Esc + 1	Help	Gives more information about the item selected. In some areas of the System Manager, you can move to the next level for more information.
F2 or Esc + 2	Refresh	Redraws the screen. Use if the console messages overwrite the screen.
F3 or Esc + 3	Previous	Returns one level to the previous screen. From the main menu, F3 (Esc + 3) will take you to the fast-path command environment.
F4 or Esc + 4 dialog screens	List	Presents a list of possible choices for an entry field. A scrollable pop-up list is displayed.
F4 or Esc + 4 menu screens	SysID	Displays a screen with high-level system configuration parameters, such as host name, serial number, model number and configuration file name.
F5 or Esc + 5	Undo	Resets the entry field to the original setting.
F6 or Esc + 6	Edit	Allows editing of an entry field. Use this key if a larger entry field is needed.
F7 or Esc + 7	Page up	Scroll to the previous page.
F8 or Esc + 8	Page down	Scroll to the next page.
F9 or Esc + 9	Select	Makes individual selections on multiple selection lists.
F10 or Esc + 0 on Main Menu	Exit	Exits the System Manager. Log in again to return.
F10 or Esc + 0 on other screens	Main Menu	Returns to the System Manager Main Menu.
Enter	Do	Performs the selected function.
Ctrl + C	Interrupt	Exits the command, when used on System Manager continuous display output screens and exits System Manager into the fast-path environment, when used on other System Manager screens. If a file is viewed from the fast-path environment using the More Facility, it exits the file.

Table 7-1 (Page 2 of 2). System Manager Function Keys

Function Key	Meaning	Description
Home or Esc + <	Top	Scroll to the top of the command output.
End or Esc + >	Bottom	Scroll to the bottom of the command output.
Page Up or Esc + V	Page up	Scrolls backward to the previous page.
Page Down or Ctrl + V	Page down	Scrolls forward to the next page.
Tab	Forward the list of options	Moves forward through a list of choices associated with a dialog item. A list of choices is denoted by a plus (+) symbol located to the right of the entry field and the absence of brackets ([]) surrounding the entry value.
Shift + Tab	Backs through the list of options	Moves backward through a list of choices associated with a dialog item. A list of choices is denoted by a plus (+) symbol located to the right of the entry field and the absence of brackets ([]) surrounding the entry value.
Arrow keys	Moves the cursor up one line or down one line	Scrolls through the information. Moves between entry fields on dialog screens. Moves the cursor beside menu items on the menu screens.
Backspace	Delete character	Deletes the character at the left of the screen.

Making Selections from a List of Choices

In the System Manager, you can make selections from one of three types of lists:

Single selection lists

Appear on selector screens.

Are available with most dialog items when you use the list option, F4 (Esc+4). It is denoted by the plus (+) symbol on a dialog screen.

Multiple selection lists

Appear with a few dialog items when you use the list option, F4 (Esc+4).

When multiple selection is available, the select option, F9 (Esc+9), is available on the selector screen.

Option rings

Appear on some dialog items.

Are denoted by the plus (+) symbol and the absence of brackets surrounding the entry field, in most instances.

Select an item from a single selection list:

1. Move the cursor to the correct item.
2. Press **Enter** to select the item.

Select more than one item from a multiple selection list:

1. Move the cursor to the first item to be selected.
2. Press **F9 (Esc + 9)** to select the individual item. Press **F9 (Esc + 9)** a second time to undo the selection.
3. Continue selecting until all desired items are highlighted.
4. Press **Enter**.

Select an item from an option ring:

1. Press **Tab** to move forward through the list of choices.
2. Press **Shift + Tab** key sequence to move backward through the list of choices.
3. Press **Enter** to select the item.

Getting System Manager Help

Help is available for System Manager screens. The type of help displayed is determined by the cursor location when you request help or by the task you are doing when you request help.

Contextual Help

Contextual help is available for dialog entry fields, selector screens, and menu items. To get contextual help, position the cursor on the entry field, list item, or menu item and press **F1 (Esc + 1)**.

On menu screens, the help information describes the task that the menu item performs. On dialog screens, the help information gives instructions for data entry in a field. On selector screens, the help information describes the list of items to select.

General Help

General help is available for the entire System Manager interface. This general help describes how to use the System Manager and the different screen types. This help is invoked from the System Manager main menu and from each of the contextual help screens, information screens and error message screens. To access this general help from the contextual help screen, the information message screen, and the error message screen, press **F1 (Esc + 1)**. There are three ways of obtaining general System Manager help from the main menu:

1. Position the cursor on the title of the System Manager main menu, **1**, and press **F1 (Esc + 1)**.
2. Position the cursor on the System Manager Help menu item, **2**, and press **F1 (Esc + 1)**.

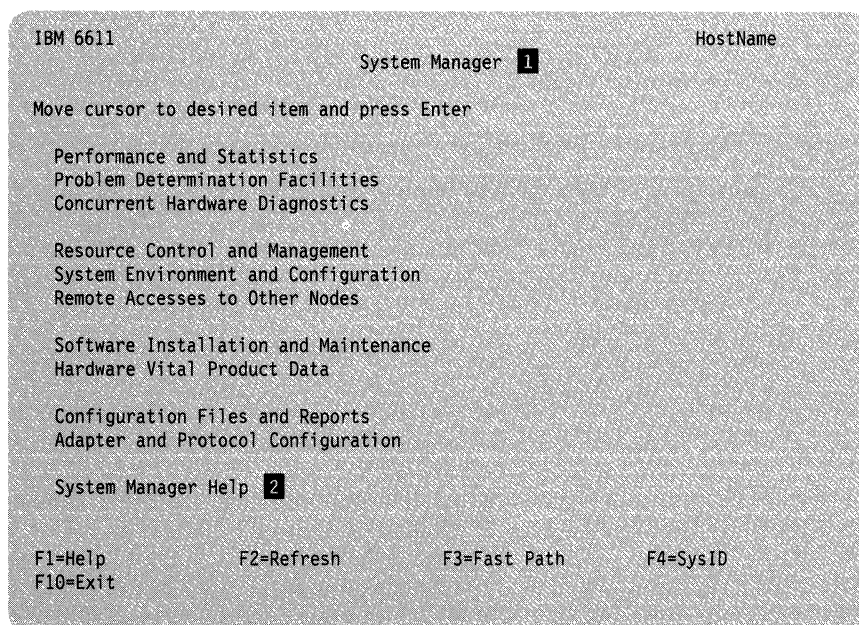


Figure 7-6. System Manager Main Menu

3. Position the cursor on the System Manager Help menu item, **2**, and press **Enter**. There is another menu from which you can select from one of five general help topics. See Figure 7-7.

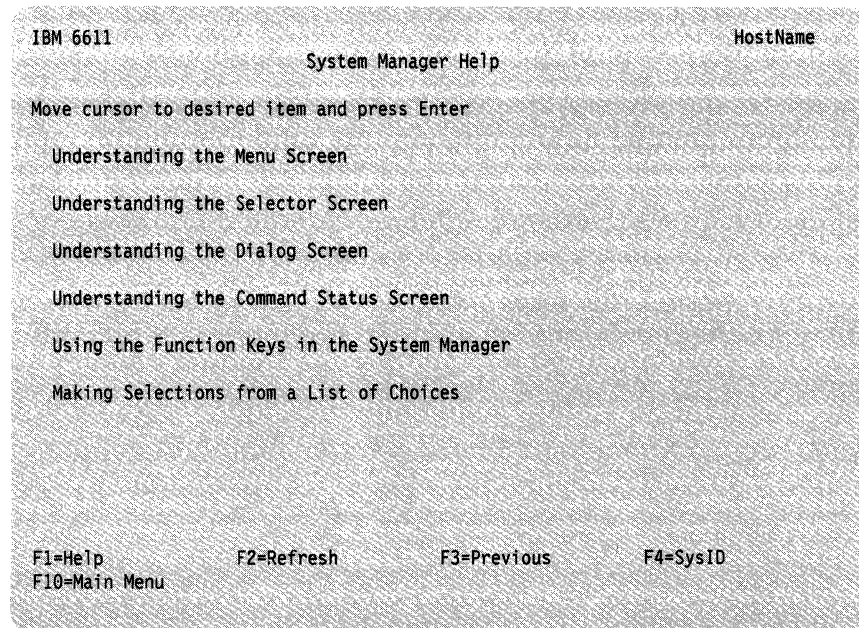


Figure 7-7. System Manager Help

To access general help, press **F4 (Esc + 4)** on a dialog entry field. This help describes the features of the pop-up list screen. To get this help, press **F1 (Esc + 1)** while viewing the list of choices.

General help is available on the field edit screen obtained by pressing **F6 (Esc + 6)** on a dialog entry field. This help describes the features of the field edit screen. To get this help, press **F1 (Esc + 1)** while viewing this screen.

General help is also available on the command status screen. To get this help, press **F1 (Esc + 1)** while viewing the command output on the command status screen.

Performing System Manager Tasks

This section provides information about the functions that the System Manager performs. Figure 7-8 shows the main menu of the System Manager. The first line of each menu screen shows the machine type in the top left corner (IBM 6611) and the host name for this IBM 6611 in the right corner.

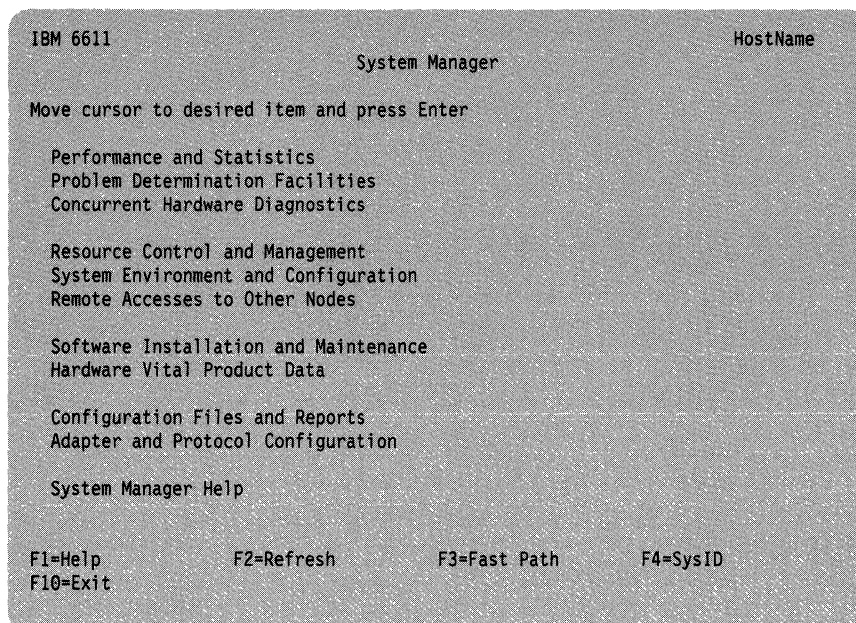


Figure 7-8. System Manager Main Menu

On the main menu, press **F3 (Esc + 3)** to go to the fast-path environment. To return to the System Manager after entering the fast-path environment by this method, type **exit** at the 6611> prompt. See “Fast-Path Environment Exit Commands” on page 8-53 for more information about the commands that will exit the fast-path environment.

Press **F10 (Esc + 0)** on all System Manager screens to exit the System Manager. When you access the IBM 6611 through the S1 or S2 serial port locally or using a modem, you exit to the login prompt by pressing **F10 (Esc + 0)**. When you access the IBM 6611 using TELNET or RLOGIN, your remote connection is closed. In order to return to the System Manager, you are required to issue the **telnet** or **rlogin** command again. For more information about how to access the System Manager, see Chapter 9.

Another way to exit the System Manager is to press **Ctrl + C**. This takes you to the fast-path command environment. You cannot return to the System Manager when you enter the fast-path environment by this method. If you type **exit**, you are logged out of the IBM 6611.

Flowchart of System Manager Menu Screens

Figure 7-9 on page 7-18 shows the navigation of the System Manager screens. Use this figure as a reference to locate System Manager tasks.

Figure 7-9 also gives the reference keys to the System Manager main menu and its menu items. Using the numbers in the shaded blocks, refer to Figure 7-10 on page 7-20 for the outline of menu items.

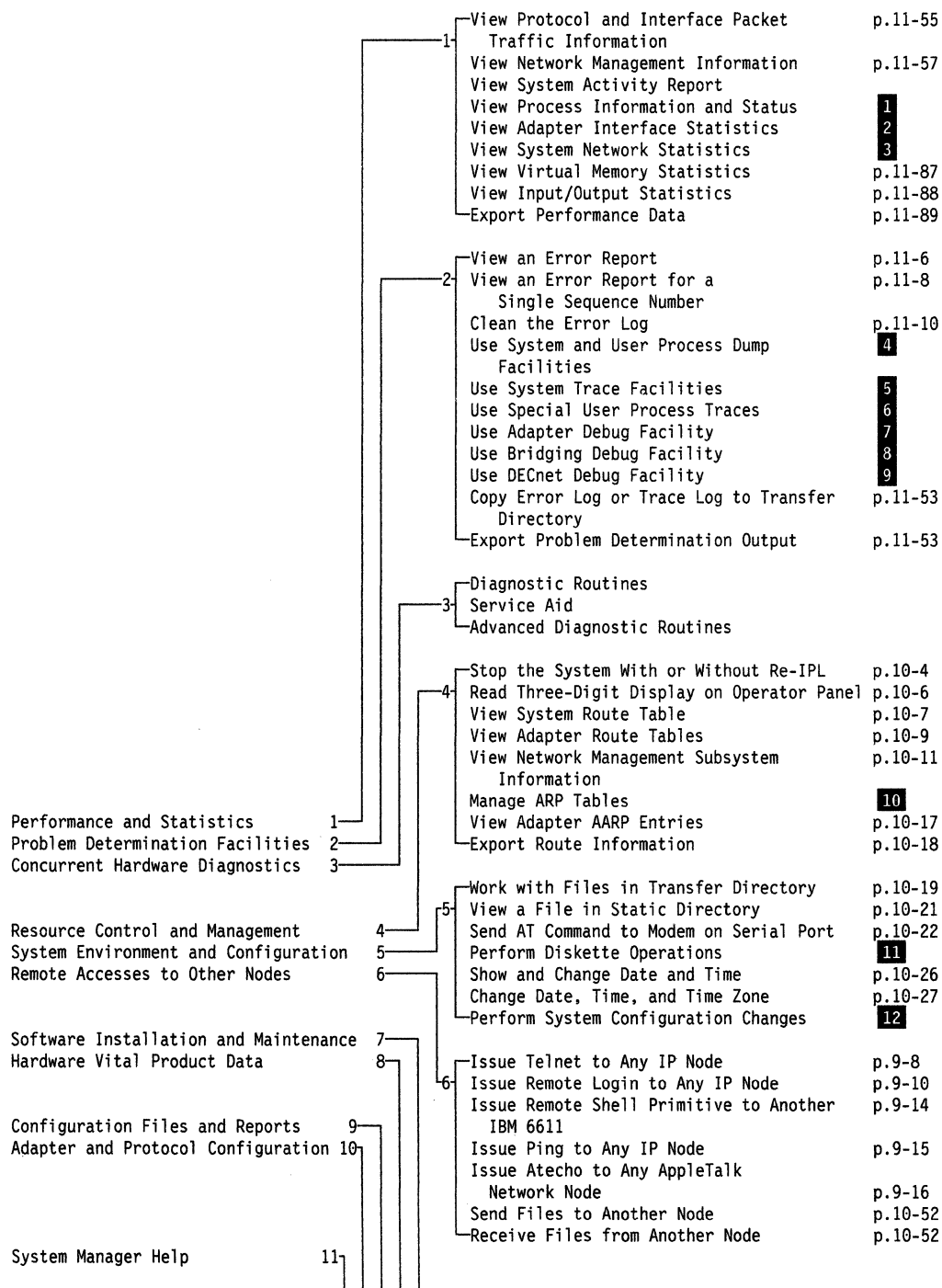


Figure 7-9 (Part 1 of 2). System Manager Menu Tree Part I

7	Import Software to Transfer Directory	p.12-7
	List All Software in the Transfer Directory	p.12-8
	List All Problems Fixed by Software Updates in the Transfer Directory	p.12-8
	Apply Software Components	p.12-12
	Apply Software Updates	p.12-9
	Restart the System After Applying New Software	p.12-13
	Clean Up After a Failed Installation	p.12-16
	List All Applied but Not Committed Software	p.12-16
	Commit Applied Updates (Delete Previous Version)	p.12-16
	Reject Applied Updates (Use Previous Version)	p.12-17
	Reinstate Saved Software Component	p.12-18
	Remove Saved Software Component	p.12-18
	View Software Vital Product Data	13
8	List All Supported Devices	p.13-9
	List All Defined Devices	p.13-10
	List All Installed Devices	p.13-11
	View Characteristics of a Defined Device	p.13-11
	View Hardware Vital Product Data	p.13-12
	Update Hardware Vital Product Data After Configuration Changes	p.13-12
	Export Hardware Vital Product Data	p.13-13
9	View Configuration Report	p.14-20
	View Configuration Error Messages	p.14-22
	View Configuration Script	p.14-23
	Import Binary Configuration File	p.14-17
	Export Binary Configuration File	p.14-17
10	Export Configuration Information	p.14-25
	Show Configuration Values for Single Object	p.14-8
	Set Configuration Values for Single Object	p.14-8
	Add Configuration Element to a List Object	p.14-8
	Delete Configuration Element from a List Object	p.14-8
	List Configuration Elements in a List Object	p.14-8
	View Configuration Report	p.14-20
	Apply Changes to Configuration Database	p.14-8
	Commit Changes to Configuration Database	p.14-8
	Reject Uncommitted Changes to Configuration Database	p.14-8
11	Understanding the Menu Screen	p.7-4
	Understanding the Selector Screen	p.7-6
	Understanding the Dialog Screen	p.7-7
	Understanding the Command Status Screen	p.7-9
	Using the Function Keys in the System Manager	p.7-11
	Making Selections from a List of Choices	p.7-13

Figure 7-9 (Part 2 of 2). System Manager Menu Tree Part I

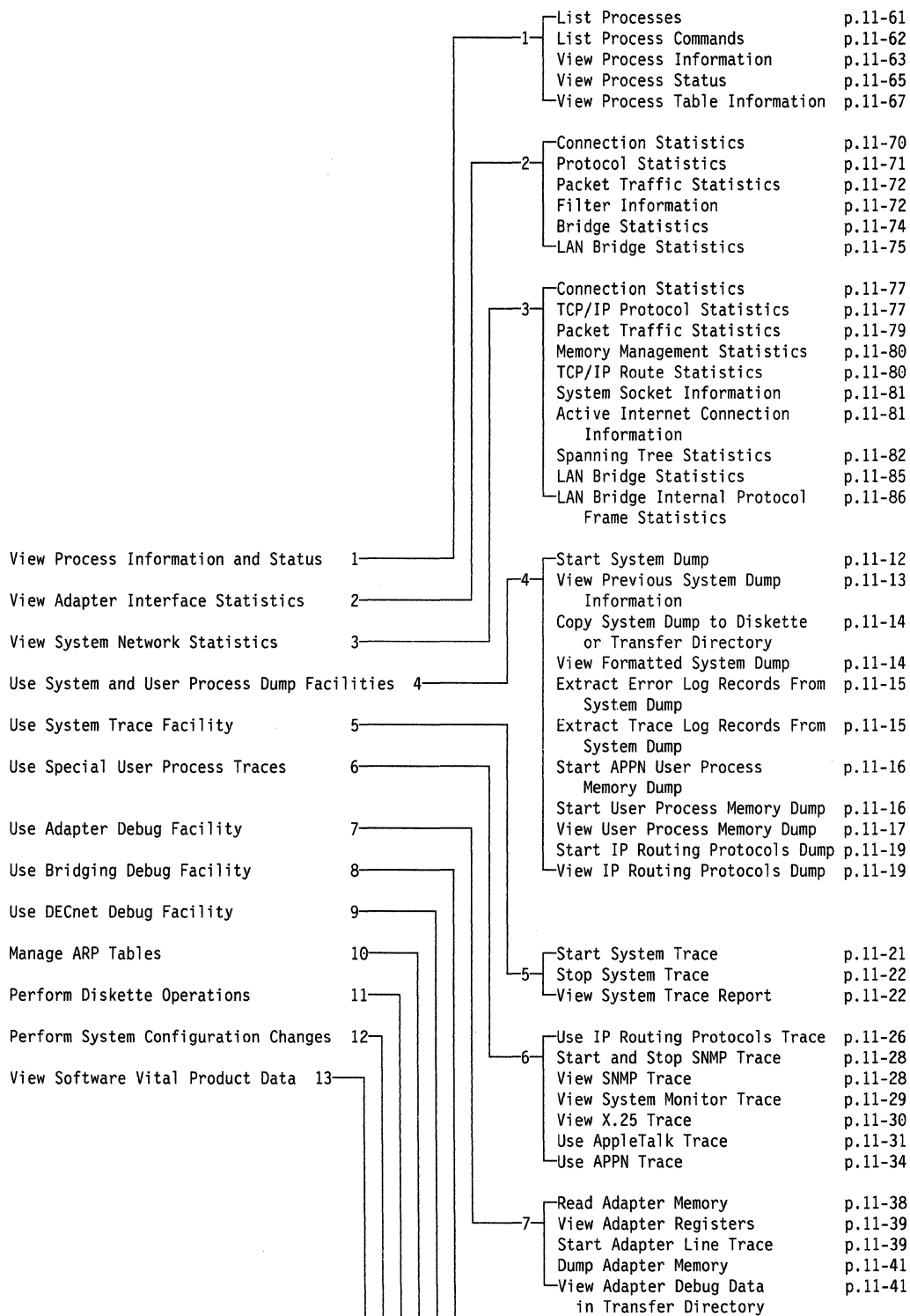


Figure 7-10 (Part 1 of 2). System Manager Menu Tree Part II

8	View Bridge Trace Files	p.11-44
	Start Bridging Frame Trace	p.11-44
	Stop Bridging Frame Trace	p.11-45
	View Bridging Frame Trace Output	p.11-45
	View Bridge Configuration Information	p.11-46
9	View Bridge SAP Filter Information	p.11-47
9	View Routing Data Structures	p.11-48
	Set DECnet Trace Log Options	p.11-50
	View DECnet Trace Output	p.11-52
10	View System ARP Entries	p.10-14
	Add System ARP Entry	p.10-14
	Delete System ARP Entry	p.10-15
	View Adapter ARP Entries	p.10-15
	Add Adapter ARP Entry	p.10-15
	Delete Adapter ARP Entry With Hardware Address	p.10-16
	Delete Adapter ARP Entry With Host Name	p.10-17
11	Clear Adapter ARP Table	p.10-17
	Format DOS Diskette	p.10-23
	List Files on DOS Diskette	p.10-24
	Import Files from DOS Diskette	p.10-24
	Export Files to DOS Diskette	p.10-25
	Format Unix Diskette	p.10-23
12	List Files on Unix Diskette	p.10-24
	Import Files from Unix Diskette	p.10-24
	Export Files to Unix Diskette	p.10-25
	Configure EIA/232 Serial Ports	p.10-30
	Configure Userids and Passwords	p.10-31
	Configure Host Name to IP Address Mapping	p.10-34
13	Configure Remote Host Name Service	p.10-37
	Configure Remote Time Service	p.10-39
	Apply Changes to Configuration Data Base	p.10-41
	Commit Changes to Configuration Data Base	p.10-42
	Reject Uncommitted Changes to Configuration Data Base	p.10-42
13	List All Installed Software	p.12-35
	List All Updates to a Software Component	p.12-35
	List Files Included in a Software Component	p.12-36
	List Prerequisites of a Software Component	p.12-36
	List Dependents of a Software Component	p.12-37
	View ID of a Software Component	p.12-38
	View History of a Software Component	p.12-38
	Verify a Software Component	p.12-39
	Export Software Vital Product Data	p.12-40

Figure 7-10 (Part 2 of 2). System Manager Menu Tree Part II

Performance and Statistics

Figure 7-11 shows the Performance and Statistics menu.

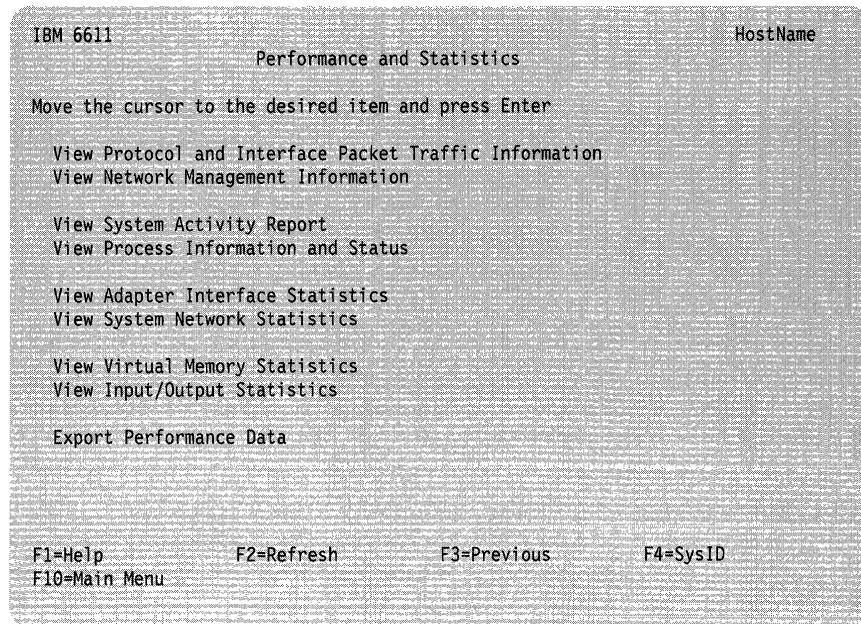


Figure 7-11. Performance and Statistics Menu

From the Performance and Statistics menu, information is gathered about the performance of many of the components in the IBM 6611, including:

- The main operating system
- The running user processes
- The installed peer-capable adapters
 - Token-Ring Network 16/4 Adapter
 - Ethernet Adapter
 - EIA 422/449 Serial Adapter
 - V.35/V.36 Serial Adapter
- The configured protocols
- The fixed disks
- The network, as viewed from both the peer-capable adapters and the main system.

The Simple Network Management Protocol (SNMP) Management Information Base (MIB) variables can also be viewed from this menu.

The output is either displayed on the screen or, in most instances, is sent to a file in the transfer directory. When the output is placed in the transfer directory, it can be sent to a diskette or transferred to a remote node. When the remote node is attached through the Internet Protocol (IP) network, the output must be sent using the File Transfer Protocol (FTP). When the IBM 6611 is accessed using a modem, the output must be sent using the Xmodem Protocol (Xmodem).

The performance data generated about most of these components is designed to be used for problem determination by IBM service personnel. When IBM service personnel are not given remote access to this IBM 6611 for problem determination, you may be asked to retrieve some of this performance data. This book does not explain or interpret the details of the performance data. However, there is a section in Chapter 11 that explains how to gather the performance data and displays

sample output from most of the performance and statistics functions. Use Table 7-2 to find the section in Chapter 11 containing the performance data you want to view or retrieve.

Table 7-2. Performance and Statistics Table

Description of Performance Data	See
Interface and protocol packet traffic monitor	"View Protocol and Interface Packet Traffic Information" on page 11-55
Network management MIB variables	"View Network Management Information" on page 11-57
System activity and statistics	"View System Activity Report" on page 11-59
Network status and statistics (adapter view)	"View Adapter Interface Statistics" on page 11-69
Network status and statistics (system view)	"View System Network Statistics" on page 11-75
System virtual memory statistics	"View Virtual Memory Statistics" on page 11-87
I/O statistics for attached terminals and fixed disks	"View Input/Output Statistics" on page 11-88

Problem Determination Facilities

Figure 7-12 shows the Problem Determination Facilities menu.

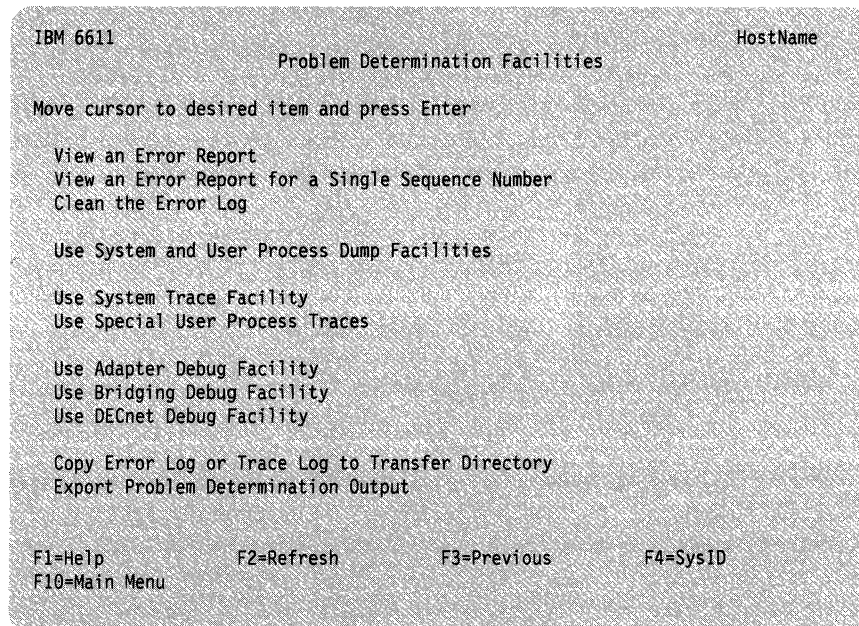


Figure 7-12. Problem Determination Facilities Menu

From the Problem Determination Facilities menu, you can perform various debugging tasks. Most of the tasks are associated with error logs, traces, and dumps. There are special facilities for debugging the peer-capable adapters, debugging the bridging protocol, and debugging the DECnet protocol.

There are three areas of the IBM 6611 to dump:

- System code
- User process code
- Adapter code.

You can issue the dump requests and view the dumped output.

There are several different traces for the IBM 6611 code:

- System Trace Facility
 - Used by the main operating system, device drivers, and some user process code to monitor system activity.
- Selected user process traces, including
 - IP Routing Protocols Trace
 - SNMP Trace
 - System Monitor Trace
 - X.25 Trace
 - AppleTalk Trace
 - APPN Trace
- Adapter line trace for incoming and outgoing data
- Bridging frame trace
- DECnet trace.

You can issue the trace start and stop requests and view the trace output.

The special debug facility for the peer-capable adapters includes the dump and trace capabilities for these adapters, as well as the ability to read adapter memory and view the adapter registers. The special bridging debug facility includes viewing trace files for LAN bridge and spanning tree and running a bridging frame trace. The DECnet debug facility includes displaying the DECnet routing data structures and setting options for and viewing the DECnet trace.

The output from most of these problem determination facilities is displayed on the screen or, in most instances, can be sent to a file in the transfer directory. When the output is placed in the transfer directory, it can be sent to a diskette or transferred to a remote node. When the remote node is attached through the IP network, the output must be sent using FTP. If the IBM 6611 is accessed via modem, the output must be sent using Xmodem.

The problem determination output generated by most of these facilities is designed for use by IBM service personnel. If IBM service personnel are not given remote access to this IBM 6611 for problem determination, you will be asked to retrieve some of this problem determination output.

Note: This book does not explain or interpret the details of the problem determination output. However, there is a section in Chapter 11 that explains how to gather the output from these problem determination facilities and displays some sample output from the facilities. Use Table 7-3 on page 7-25 to find the section in Chapter 11 containing the problem determination output you want to view or retrieve.

Table 7-3. Problem Determination Facilities Table

Problem Determination Data to Gather	See
Error report	"Generating an Error Report" on page 11-6
System dump	"Start System Dump" on page 11-12
Formatted system dump	"Start System Dump" on page 11-12
User process dump	"Start User Process Memory Dump" on page 11-16
APPN dump	"Start APPN User Process Memory Dump" on page 11-16
IP routing protocols dump	"Start IP Routing Protocols Dump" on page 11-19
System trace report	"Use System Trace Facility" on page 11-21
IP routing protocols trace output	"Start IP Routing Protocols Trace" on page 11-25
SNMP trace output	"Start and Stop SNMP Trace" on page 11-28
System monitor trace output	"View System Monitor Trace" on page 11-29
X.25 trace output	"View X.25 Trace" on page 11-30
AppleTalk trace output	"Use AppleTalk Trace" on page 11-31
APPN trace output	"Use APPN Trace" on page 11-34
Adapter debug facility output	"Use Adapter Debug Facility" on page 11-37
Bridging debug facility output	"Use Source Route Bridging Debug Facility" on page 11-42
DECnet debug facility output	"Use DECnet Debug Facility" on page 11-48

Concurrent Hardware Diagnostics

All of the menu items on the main menu lead to another menu screen or group of menu screens for the System Manager, except for Concurrent Hardware Diagnostics. If you select the Concurrent Hardware Diagnostics menu item, control is passed to the Hardware Diagnostics Facility. You are no longer in the System Manager.

Concurrent hardware diagnostics are diagnostics that can be run while the system is in operation. They are designed to test as much of the system, or specified resource, as possible without interfering with system operations. This is the only type of diagnostics that can be run from the System Manager.

When you select Concurrent Hardware Diagnostics from the System Manager main menu, the next screen that appears is Diagnostic Operating Instructions. See Figure 7-13 on page 7-26. Press **Enter** to proceed to the Function Selection menu. See Figure 7-14 on page 7-26. See page 13-2 for more details about concurrent hardware diagnostics. For information about stand-alone diagnostics, refer to the *IBM 6611 Network Processor Installation and Service Guide*.

LICENSED MATERIALS - PROPERTY OF IBM.
IBM 6611 Network Processor DIAGNOSTICS VERSION 1.0
(C) COPYRIGHTS BY IBM AND BY OTHERS 1982, 1992.
ALL RIGHTS RESERVED.
US GOVERNMENT USERS RESTRICTED RIGHTS -
USE, DUPLICATION OR DISCLOSURE RESTRICTED
BY GSA ADP SCHEDULE CONTRACT WITH IBM CORP.

DIAGNOSTIC OPERATING INSTRUCTIONS

These program contain diagnostics and service aids for the system. These procedures should be used whenever problems with the system occur which have not been corrected by any software application procedures available. In general, the procedures will run automatically. However, sometimes you will be required to select options, inform the system when to continue, do simple tasks, and exchange diskettes.

Several keys are used to control the procedures:

- The Enter key continues the procedure or performs an action
- The Backspace key allows keying errors to be corrected.
- The cursor keys are used to select an option.

Press the F3 key to exit or press Enter to continue.

Figure 7-13. Diagnostic Operating Instructions Screen

FUNCTION SELECTION

Move the cursor to selection, then press Enter.

Diagnostic Routines

This selection will test the machine hardware and detect any hardware problems. A problem will be indicated by a SRN (Service Request Number). The SRN will allow a service representative to quickly determine what parts are required to repair the machine.

Service Aid

This selection will look at the machine configuration, exercise external interfaces, format media, look at past diagnostic results, control what resources are tested, check out media, etc.

Advanced Diagnostic Routines

This selection will normally be used by the service representative.

F3=Cancel

F7=Page Up

F8=Page Down

F10=Exit

Figure 7-14. Function Selection Menu

Resource Control and Management

Figure 7-15 shows the Resource Control and Management menu.

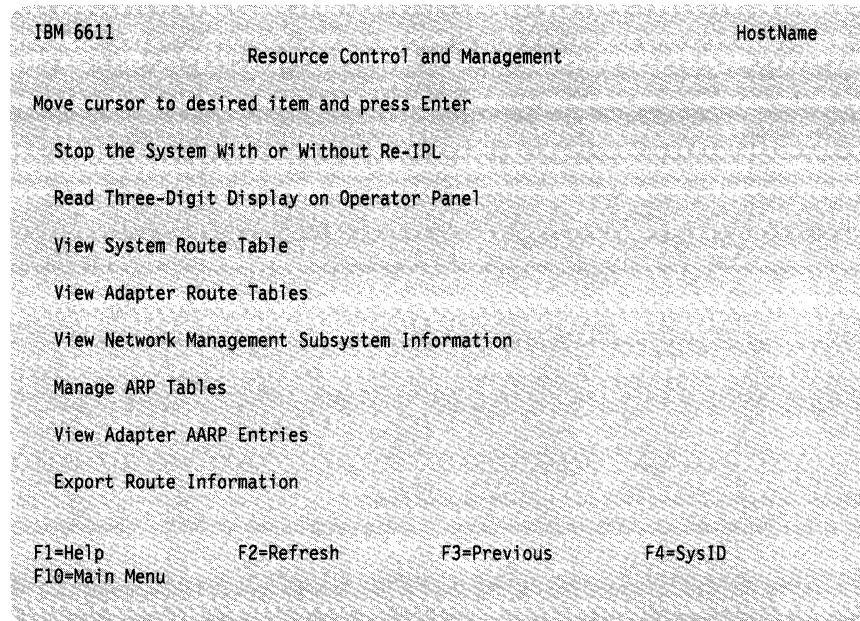


Figure 7-15. Resource Control and Management Menu

From the Resource Control and Management menu, you can stop the IBM 6611, and optionally restart it in one step. There is a three-digit display on the operator panel of the IBM 6611 that displays error and status codes at various times during IBM 6611 operation. The values displayed can be read remotely from the IBM 6611 using the System Manager.

You can display the system route table and the peer-capable adapter route tables. Special network management subsystem information can be viewed.

You can add or delete entries to the IP Address Resolution Protocol (ARP) tables and list the tables. There are IP ARP tables in the base operating system and on the peer-capable adapters. You can view the AppleTalk ARP (AARP) table in the base operating system.

The route tables are either displayed on the screen or can be sent to a file in the transfer directory. When the table is placed in the transfer directory, it can be sent to a diskette or transferred to a remote node. If the remote node is attached through the IP network, the route table must be sent using FTP. When the IBM 6611 is accessed using a modem, the route table must be sent using Xmodem.

Each of these management tasks is discussed in more detail in Chapter 10. Use Table 7-4 on page 7-28 to locate the additional discussion on performing these tasks.

Table 7-4. Resource Control and Management Table

Description of Management Task	See
Stopping the IBM 6611	"Stopping the IBM 6611" on page 10-4
Reading the 3-digit display	"Reading the Three-Digit Display" on page 10-6
Viewing system route table	"Viewing the System Route Table" on page 10-7
Viewing adapter route tables	"Viewing the Adapter Route Tables" on page 10-9
Viewing network management subsystem information	"Viewing the Network Management Subsystem Information" on page 10-11
Managing ARP tables	"Managing ARP Tables" on page 10-13
View adapter AARP table	"Viewing Adapter AARP Entries" on page 10-17

System Environment and Configuration

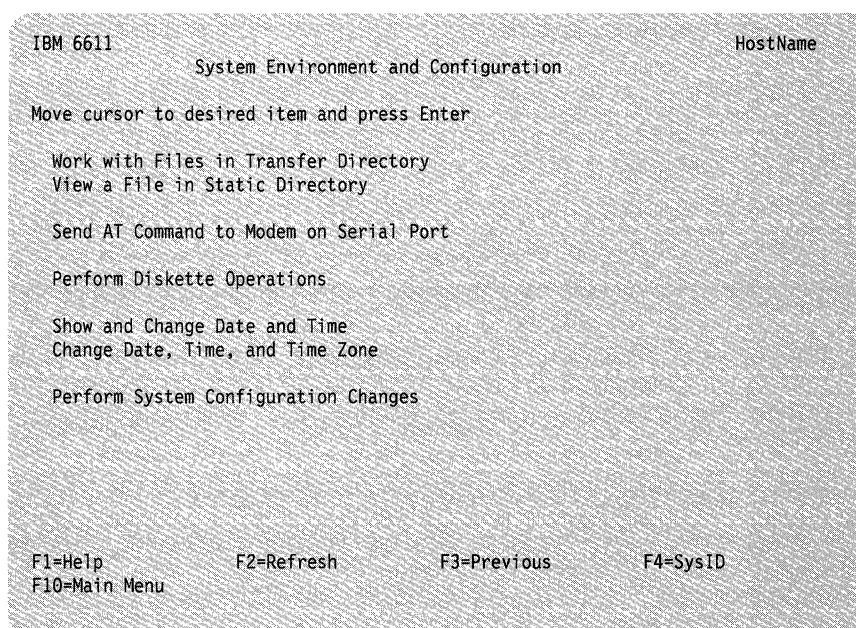


Figure 7-16. System Environment and Configuration Menu

Figure 7-16 shows the System Environment and Configuration menu. From the System Environment and Configuration menu and the two lower level menus, Perform Diskette Operations and Perform System Configuration Changes, you can perform various system operational tasks. You can set the time, date, and time zone, if needed. You can configure the EIA 232 S1 or S2 serial port and send an AT command to an attached modem. You can view files in the static directory and view, rename, or delete files in the transfer directory.

You can perform diskette operations with either DOS or UNIX** diskettes, including:

- Formatting the diskette
- Listing the files on the diskette
- Importing the files from the diskette
- Exporting the files to the diskette.

Some of the system configuration functions that are available are as follows:

- Setting userids and passwords
- Setting this IBM 6611's host and domain name
- Setting up a table of remote host names mapped to their IP addresses
- Enabling remote name service and remote time service.

Each of these tasks is discussed in more detail in Chapter 10. Use Table 7-5 to locate the additional discussion on performing these tasks.

Table 7-5. System Environment Table

Description of System Task	See
Working with files in transfer directory	"Working with Files in the Transfer Directory" on page 10-19
Viewing a file in the static directory	"Viewing a File in the Static Directory" on page 10-21
Sending an AT command to a modem attached to a serial port	"Sending an AT Command to a Modem Attached to an EIA 232 Serial Port" on page 10-22
Formatting the diskette	"Formatting a DOS or UNIX Diskette" on page 10-23
Listing the files on the diskette	"Listing Files on a DOS or UNIX Diskette" on page 10-24
Importing the files from the diskette	"Importing Files From a DOS or UNIX Diskette" on page 10-24
Exporting the files to the diskette	"Exporting Files to a DOS or UNIX Diskette" on page 10-25
Showing and changing date and time	"Showing and Changing the Date and Time" on page 10-26
Changing date, time, and time zone	"Changing the Date, Time, and Time Zone" on page 10-27
Configuring EIA 232 serial ports	"Configuring the EIA 232 S1 and S2 Serial Ports" on page 10-30
Adding or deleting userids and passwords	"Configuring Userids and Passwords" on page 10-31
Setting up a host name and a domain name for this IBM 6611.	"Configuring Host Name to IP Address Mapping" on page 10-34
Configuring host name to IP address mapping	"Configuring Host Name to IP Address Mapping" on page 10-34
Configuring remote host name service	"Configuring Remote Host Name Service" on page 10-37
Configuring remote time service	"Configuring Remote Time Service" on page 10-39

Remote Accesses to Other Nodes

Figure 7-17 shows the Remote Accesses to Other Nodes menu.

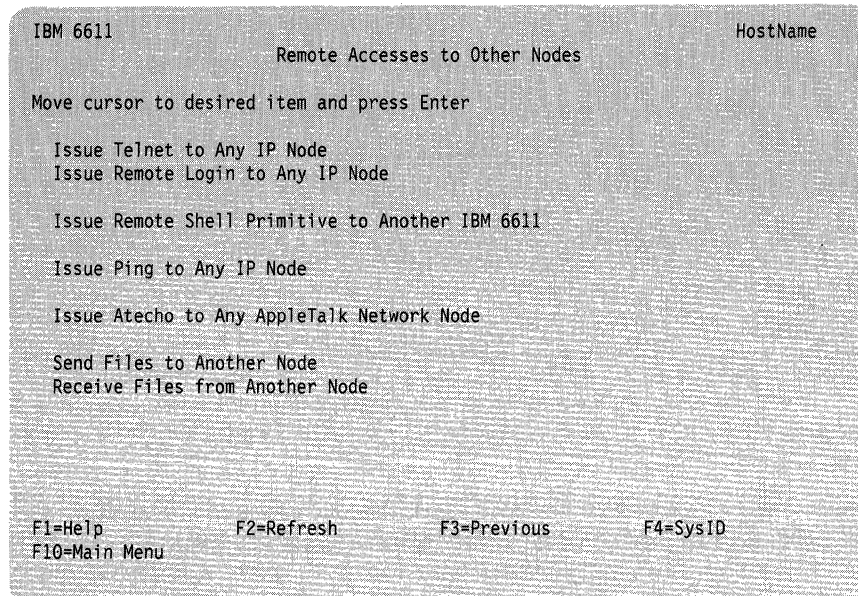


Figure 7-17. Remote Accesses to Other Nodes

From the Remote Accesses to Other Nodes menu, you can establish a remote interactive session between this IBM 6611 and another IBM 6611 or another IP node using either the **telnet** or the remote login (**rlogin**) command. You need to specify the host name (or IP address) and a userid and password at the remote node. The remote IP node must support the **telnet** or **rlogin** command.

You can issue single commands from this IBM 6611 to another IBM 6611 using the remote shell (**rsh**) command. You need to specify the host name (or IP address) and a userid and password at the remote IBM 6611. The **rsh** command is designed to work from within a UNIX shell.

You can test for the ability to reach another IBM 6611 or other IP node from this IBM 6611 using the Internet Control Message Protocol (**ping** command). You can test the ability to reach another node on the AppleTalk network from this IBM 6611 by using the **atecho** command.

This menu can also be used to transfer files between this IBM 6611 and another IBM 6611 or other IP node using FTP. You can transfer files between this IBM 6611 and another node attached through a modem and the public switched network using Xmodem. Files can be sent from either the transfer directory or the static directory. Files are received into the transfer directory.

Each of these tasks is discussed in more detail in Chapter 9 or Chapter 10. Use Table 7-6 on page 7-31 to locate the additional discussion on performing these tasks.

Table 7-6. Remote Accesses to Other Nodes Table

Description of Access Method	See
telnet	"Using TELNET" on page 9-8
rlogin	"Using Remote Login" on page 9-10
rexec	"Using Remote Execution" on page 9-13
rsh	"Using Remote Shell" on page 9-14
ping	"Using Ping" on page 9-15
atecho	"Using Atecho for AppleTalk" on page 9-16
Sending or receiving files using FTP	"Using the File Transfer Protocol" on page 10-52
Sending or receiving files using Xmodem	"Using the Xmodem Protocol" on page 10-55

Software Installation and Maintenance

Figure 7-18 shows the Software Installation and Maintenance menu.

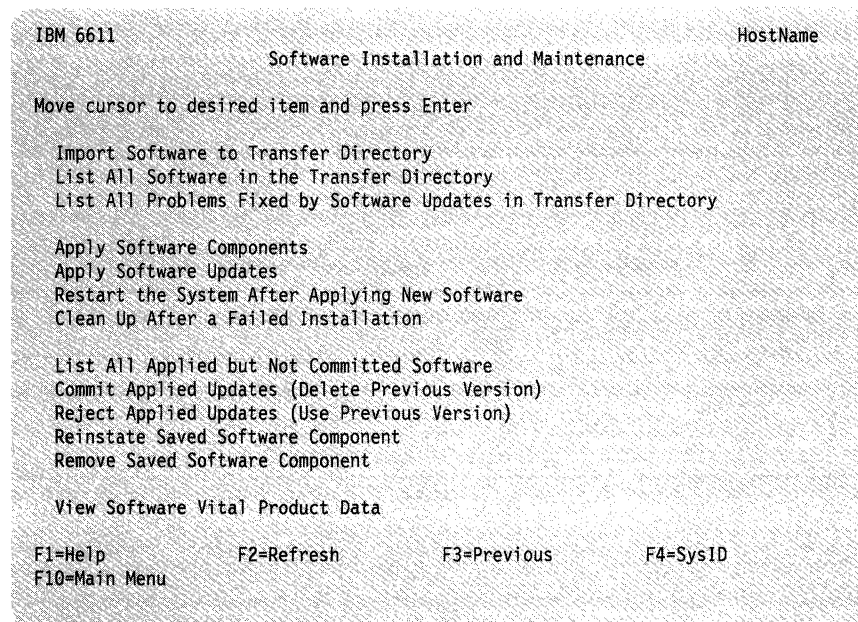


Figure 7-18. Software Installation and Maintenance Menu

From the Software Installation and Maintenance menu, you can perform each of the tasks associated with installing the Multiprotocol Network Program and updates to the Multiprotocol Network Program. These tasks are performed with the Software Installation and Maintenance facility. The software updates are distributed in the form of program temporary fixes (PTFs).

All incoming software components and updates can be installed from either the transfer directory or a diskette. You can view the software components and updates in the transfer directory and see which problems are fixed with which software update.

You will receive software components to install, software updates to install, or both. If you receive both, they are installed separately. Use the following tasks to install the software:

- Apply software components
- Apply software updates.

You can choose to install all the software updates at once or individually select the updates you want to install, as long as prerequisite software is installed first. The IBM 6611 must be **restarted** after installing the software. When you install a new software component, the existing one is saved. It can be reinstated if the new component is unacceptable or removed to save space.

After the software updates have been installed and tested, they can be committed or rejected. If there is a failure with the installation, there is the ability to perform a clean-up operation.

You can view the software vital product data (VPD). There is a separate menu for this task, because of the many ways of viewing this data. Figure 7-19 shows the View Software Vital Product Data menu.

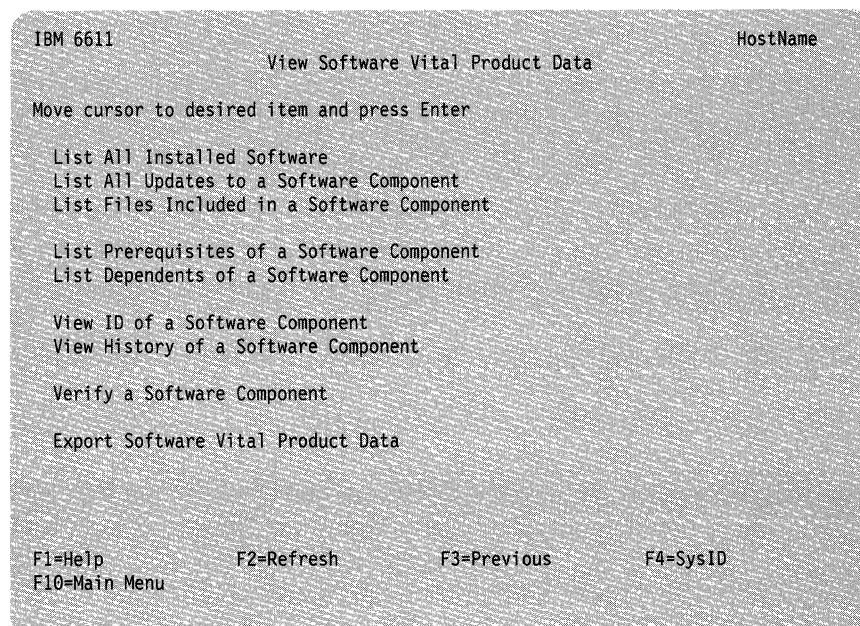


Figure 7-19. View Software Vital Product Data Menu

The software VPD is displayed on the screen or can be sent to a file in the transfer directory. When the VPD is placed in the transfer directory, it can be sent to a diskette or transferred to a remote node. If the remote node is attached through the IP network, the VPD must be sent using FTP. If the IBM 6611 is accessed using a modem, the VPD must be sent using Xmodem.

There is a detailed discussion about installing the IBM 6611 software components and their updates in Chapter 12. Chapter 12 also includes information about gathering the software VPD and displaying software VPD output. Use Table 7-7 on page 7-33 to locate a specific discussion on software installation and software VPD.

Table 7-7. Software Installation and Maintenance Table

Description of installation or maintenance task	See
Import software to transfer directory	"Transferring Software Changes to an IBM 6611" on page 12-25
List all software updates in the transfer directory	"List All Software in the Transfer Directory" on page 12-8
List all problems fixed by software updates	"List All Problems Fixed by Software Updates in Transfer Directory" on page 12-8
Apply software component	"Apply Software Components" on page 12-12
Apply software updates	"Apply Software Updates" on page 12-9
Clean up after a failed installation	"Clean Up After a Failed Installation" on page 12-16
Restart IBM 6611 after applying new software	"Restart System After Applying New Software" on page 12-13
List all software applied but not committed	"List All Applied but Not Committed Software" on page 12-16
Commit applied updates	"Commit Applied Updates (Delete Previous Version)" on page 12-16
Reject applied updates	"Reject Applied Updates (Use Previous Version)" on page 12-17
Reinstate saved software components	"Reinstate Saved Software Component" on page 12-18
Remove saved software components	"Remove Saved Software Component" on page 12-18
List all installed software	"List All Installed Software" on page 12-35
List all updates to a software component	"List All Updates to a Software Component" on page 12-35
List files included in a software component	"List Files Included in a Software Component" on page 12-36
List prerequisites of a software component	"List Prerequisites of a Software Component" on page 12-36
List dependents of a software component	"List Dependents of a Software Component" on page 12-37
View ID of a software component	"View ID of a Software Component" on page 12-38
View history of a software component	"View History of a Software Component" on page 12-38
Verify a software component	"Verify a Software Component" on page 12-39

Hardware Vital Product Data

Figure 7-20 shows the Hardware Vital Product Data menu.

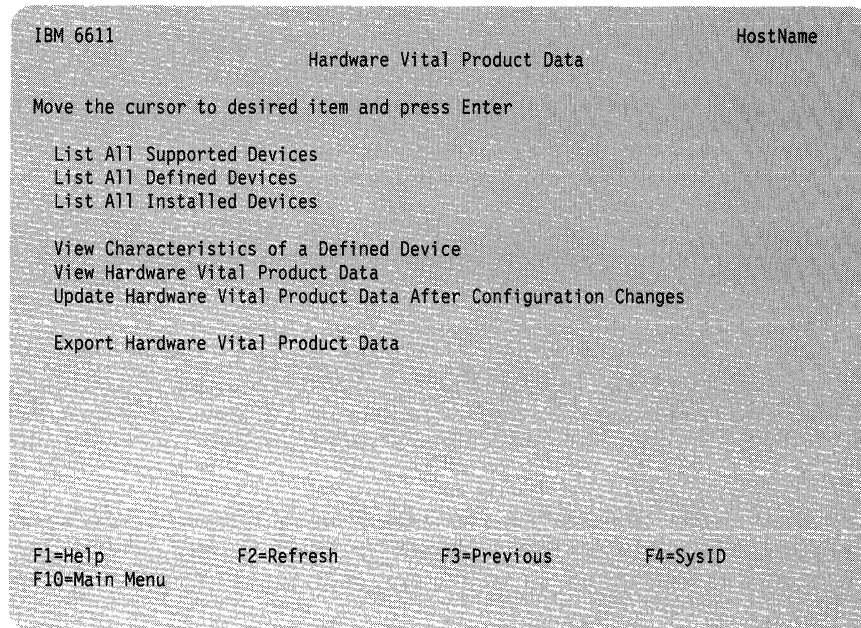


Figure 7-20. Hardware Vital Product Data Menu

From the Hardware Vital Product Data menu, you can:

- List supported, defined, and installed devices
- View characteristics of a defined device
- View hardware VPD
- Update hardware VPD after configuration changes.

The hardware VPD is displayed on the screen or can be sent to a file in the transfer directory. When the VPD is placed in the transfer directory, it can be sent to a diskette or transferred to a remote node. If the remote node is attached through the IP network, the VPD must be sent using FTP. If the IBM 6611 is accessed using a modem, the VPD must be sent using Xmodem.

There is a detailed discussion in Chapter 13 about the components of hardware VPD. It includes steps for gathering the data and shows sample hardware VPD. Use Table 7-8 on page 7-35 to locate the additional discussion on hardware VPD.

Table 7-8. Hardware VPD

Description of hardware VPD	See
List of all supported devices	"Listing Supported Devices" on page 13-9
List of all defined devices	"Listing Defined Devices" on page 13-10
List of all installed devices	"List All Installed Devices" on page 13-11
Characteristics of a defined device	"View Characteristics of a Defined Device" on page 13-11
Detailed hardware VPD for installed devices	"Viewing Hardware Vital Product Data" on page 13-12
Hardware VPD update for configuration changes	"Updating the Hardware VPD after Configuration Changes" on page 13-12
Export Hardware VPD	"Exporting the Hardware Vital Product Data" on page 13-13

Configuration Files and Reports

Figure 7-21 shows the Configuration Files and Reports menu.

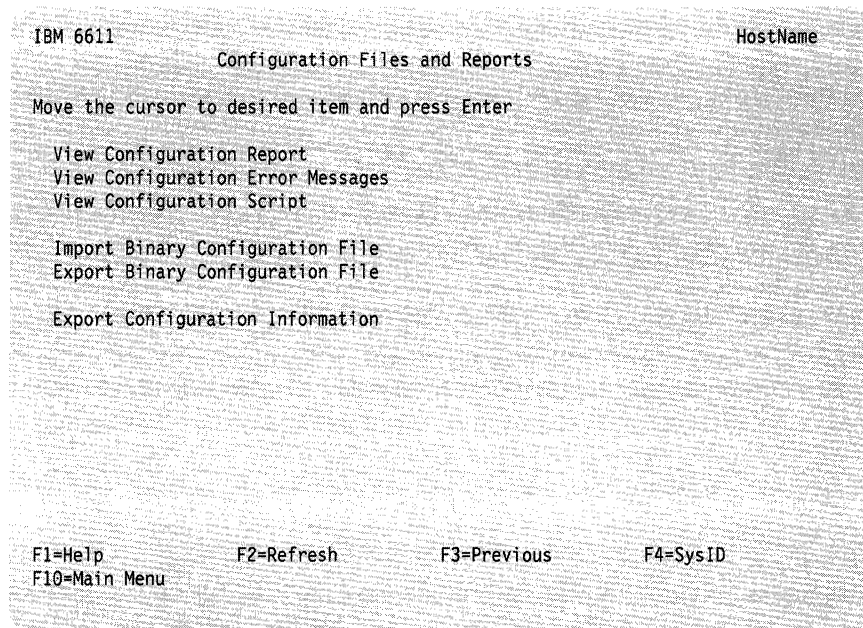


Figure 7-21. Configuration Files and Reports Menu

From the Configuration Files and Reports menu, you can view the configuration report, the configuration error messages, and the configuration script. You can import the binary configuration file to the IBM 6611 and make it the new configuration. This binary configuration file can also be exported from the IBM 6611.

The configuration report contains the current values of each of the configured configuration parameters. The configuration error messages are sent to the IBM 6611 Error Log by the configuration processor and the protocol, adapter, and system code that check for valid parameter values. A configuration error report can be generated from these messages. Whenever the System Manager is used to update a configuration, a history of commands issued is retained in the configuration script.

The configuration report, script, and error message reports are either displayed on the screen or can be sent to a file in the transfer directory. When the reports are placed in the transfer directory, they can be sent to a diskette or transferred to a remote node. If the remote node is attached through the IP network, the reports must be sent using FTP. If the IBM 6611 is accessed using a modem, the reports must be sent using Xmodem.

The details of the configuration management tasks performed by the System Manager are in Chapter 14. There is also sample output from the configuration report, the configuration script, and the configuration error report. Use Table 7-9 to locate the additional discussion on configuration management tasks.

Table 7-9. System Configuration Management Table

Configuration management task	See
View configuration report	"Configuration Report" on page 14-20
View configuration error messages	"Configuration Error Message Report" on page 14-22
View configuration script	"Configuration Script" on page 14-23.
Import binary configuration file	"Importing and Exporting the Configuration File" on page 14-17
Export binary configuration file	"Importing and Exporting the Configuration File" on page 14-17

Adapter and Protocol Configuration

An alternate way to configure the IBM 6611 is with the System Manager. This method should be used only when the Configuration Program is not available.

Most of the configuration parameters that exist in the Configuration Program also exist in the dialogs under the Adapter and Protocol Configuration menu. However, there is little error checking with this method. There are no checks to ensure that you configure each parameter that is dependent on another parameter, or values that are interdependent. This method of configuring the IBM 6611 is used only by the IBM service personnel, who have an extensive knowledge of the interdependencies of the configuration parameters.

To enter the System Manager configuration facility, select the Adapter and Protocol Configuration menu item from the main menu. The first screen you receive is a warning screen, shown in Figure 7-22 on page 7-37. Press **Enter** to go to the main Adapter and Protocol Configuration menu. This screen is shown in Figure 7-23 on page 7-37.

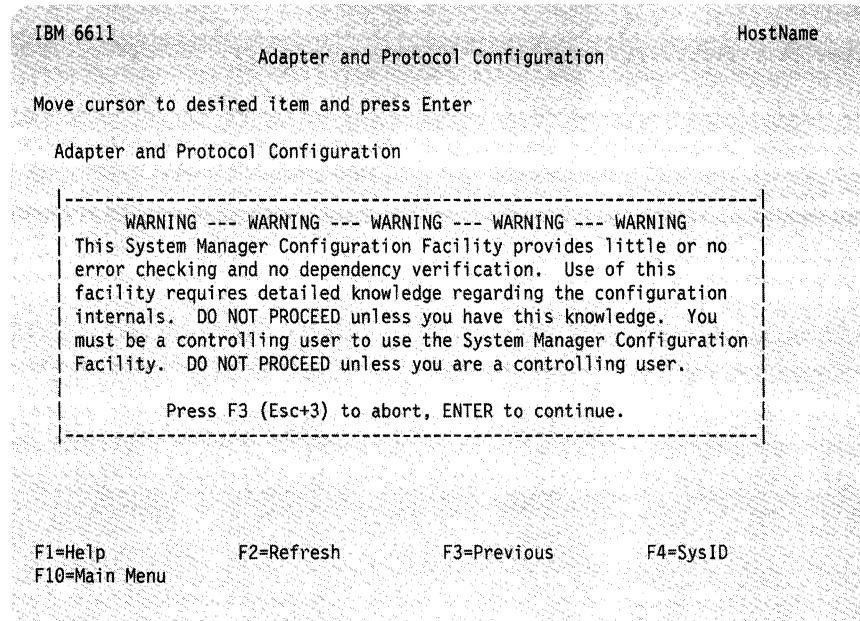


Figure 7-22. Adapter and Protocol Configuration Screen 1

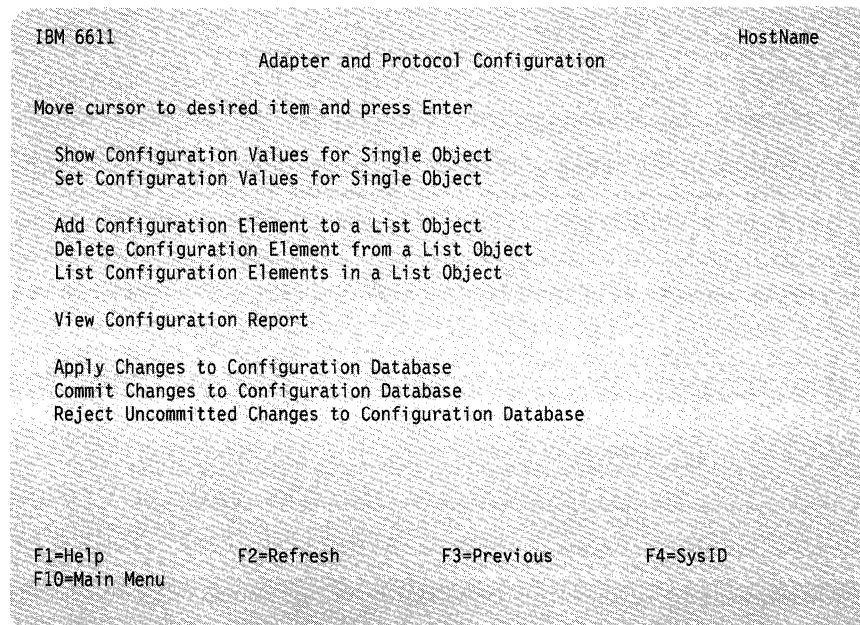


Figure 7-23. Adapter and Protocol Configuration Screen 2

Chapter 8. Using the Fast-Path Environment and Command Primitives

Introduction	8-6
Executing the Command Primitives	8-6
Accessing the Fast-Path Environment	8-7
Exiting the Fast-Path Environment	8-7
Getting Help in the Fast-Path Environment	8-8
Adapter Debug Facility Command Primitives	8-10
adp_dump	8-10
adp_line_trc_start	8-10
adp_name_list	8-10
adp_read_mem	8-11
adp_show_regs	8-11
Address Resolution Protocol: Adapter Command Primitives	8-12
aarp_adp_list	8-12
arp_adp_add_perm_nopub	8-12
arp_adp_add_perm_pub	8-12
arp_adp_add_temp_nopub	8-13
arp_adp_add_temp_pub	8-13
arp_adp_del_addr	8-13
arp_adp_del_host	8-14
arp_adp_flush	8-14
arp_adp_list	8-14
interface_list	8-15
Address Resolution Protocol: System Command Primitives	8-16
arp_hw_type_list	8-16
arp_sys_add_perm_nopub	8-16
arp_sys_add_perm_pub	8-16
arp_sys_add_temp_nopub	8-17
arp_sys_add_temp_pub	8-17
arp_sys_del_host	8-17
arp_sys_list	8-18
Bridging Debug Facility Command Primitives	8-19
brdg_cfg_info	8-19
brdg_sap_filter	8-19
port_list	8-19
stat_adp_brdg	8-20
stat_adp_lanbr	8-20
stat_srb_sptree	8-20
stat_srb_sptree_frm	8-21
stat_sys_lanbr	8-21
stat_sys_lanbr_frm	8-21
stat_tb_sptree	8-22
stat_tb_sptree_frm	8-22
trace_brdg_start	8-22
trace_brdg_stop	8-23
trace_brdg_view	8-24
Configuration Command Primitives	8-25
config_app	8-25
config_com	8-25
config_err_rpt	8-25
config_file_run	8-26
config_list	8-26

config_reinstate	8-26
config_rej	8-27
config_rpt	8-27
config_script	8-27
config_sysid	8-28
DECnet Debug Facility Command Primitives	8-29
dec_adj	8-29
dec_area_cost	8-29
dec_area_hop	8-30
dec_area_min_cost	8-30
dec_area_min_hop	8-31
dec_area_out_adj	8-31
dec_area_reach	8-32
dec_circuit	8-32
dec_cost	8-33
dec_executor	8-33
dec_hop	8-33
dec_min_cost	8-34
dec_min_hop	8-34
dec_out_adj	8-34
dec_reach	8-35
trace_dec_level	8-35
trace_dec_log	8-36
trace_dec_mask	8-36
trace_dec_time	8-36
Diskette Command Primitives	8-37
disk_dwn_files_dos	8-37
disk_dwn_files_unix	8-37
disk_format_dos_hi	8-37
disk_format_dos_low	8-38
disk_format_unix_hi	8-38
disk_format_unix_low	8-38
disk_list_files_dos	8-38
disk_list_files_unix	8-39
disk_up_files_dos	8-39
disk_up_files_unix	8-39
Dump: System Command Primitives	8-40
dump_ex_err_log	8-40
dump_ex_trc_log	8-40
dump_prev_info	8-40
dump_system	8-40
dump_system_format	8-41
dump_system_trans	8-41
Dump: User Process Command Primitives	8-42
dump_appn	8-42
dump_iproto	8-42
dump_process	8-42
proc_list	8-42
Error Report Command Primitives	8-43
err_id_list	8-43
err_log_trans	8-43
err_rpt_det	8-43
err_rpt_eid_det	8-44
err_rpt_eid_sum	8-44
err_rpt_etype_det	8-45
err_rpt_etype_sum	8-45

err_rpt_hw_det	8-46
err_rpt_hw_rsc_det	8-46
err_rpt_hw_rsc_sum	8-47
err_rpt_hw_sum	8-47
err_rpt_op_det	8-48
err_rpt_op_sum	8-48
err_rpt_seq	8-49
err_rpt_sum	8-49
err_rpt_sw_det	8-49
err_rpt_sw_rsc_det	8-50
err_rpt_sw_rsc_sum	8-50
err_rpt_sw_sum	8-51
err_type_list	8-51
hw_rsc_list	8-52
seq_num_list	8-52
sw_rsc_list	8-52
Fast-Path Environment Exit Commands	8-53
exit	8-53
quit	8-53
File Management Command Primitives	8-54
files_clr_all_trans	8-54
files_clr_one_trans	8-54
files_list_static	8-54
files_list_trans	8-55
files_rename_trans	8-55
files_view_static	8-55
files_view_trans	8-56
Hardware Command Primitives	8-57
hw_cfg_chg	8-57
hw_def_list	8-57
hw_detail	8-57
hw_diag	8-57
hw_diag_list	8-58
hw_install_list	8-58
hw_serial_model	8-58
hw_sup_list	8-59
hw_vpd_list	8-59
Host Name Command Primitives	8-60
host_name_set	8-60
host_name_show	8-60
Host Name to IP Address Mapping Command Primitives	8-61
map_host_add	8-61
map_host_del	8-61
map_host_list	8-61
Install Command Primitives	8-62
install_cleanup	8-62
install_comp	8-62
install_fix_list	8-62
install_not_commit_list	8-63
install_reinstate_saved_comp	8-63
install_remove_saved_comp	8-63
install_sw_list	8-63
install_up_trans	8-64
install_upd	8-64
install_upd_commit	8-64
install_upd_reject	8-64

install_verify	8-65
Name Server Command Primitives	8-66
name_serv_add	8-66
name_serv_del	8-66
name_serv_list	8-66
name_serv_start	8-67
name_serv_stop	8-67
Process Command Primitives	8-68
proc_command	8-68
proc_info	8-68
proc_list	8-68
proc_stat	8-68
proc_table	8-69
Remote Access Commands	8-70
atecho	8-70
ftp	8-70
modem_rcv	8-70
modem_send	8-71
ping	8-71
rlogin	8-71
telnet	8-72
Route Table Command Primitives	8-73
interface_list	8-73
route_adp_table	8-73
route_sys_table	8-73
Serial Port Command Primitives	8-74
modem_rcv	8-74
modem_send	8-74
s1_at	8-74
s1_baud	8-75
s2_at	8-75
s2_baud	8-75
Shutdown: System Command Primitives	8-76
shutdown_at_ipl	8-76
shutdown_at_noipl	8-76
shutdown_soon_ipl	8-76
shutdown_soon_noipl	8-77
Software Lock Primitive	8-78
sw_lock	8-78
Software VPD Command Primitives	8-79
sw_dep_list	8-79
sw_files_list	8-79
sw_history	8-79
sw_id	8-79
sw_list	8-80
sw_prereq	8-80
sw_upd_list	8-80
Statistic-Gathering Command Primitives	8-81
interface_list	8-81
stat_adp_con	8-81
stat_adp_filter	8-81
stat_adp_pack_traf	8-81
stat_adp_proto	8-82
stat_adp_proto_mon	8-82
stat_inet	8-82
stat_io	8-83

stat_mem_man	8-83
stat_net_con	8-83
stat_route	8-83
stat_socket	8-84
stat_sys_activity	8-84
stat_sys_pack_traf	8-84
stat_sys_proto	8-85
stat_virt_mem	8-85
Terminal Control Primitives	8-86
set_backspace	8-86
set_interrupt	8-86
Time Server Command Primitives	8-87
time_serv_add	8-87
time_serv_del	8-87
time_serv_list	8-87
time_serv_start	8-88
time_serv_stop	8-88
Time: System Command Primitives	8-89
time_date_set	8-89
time_zone_set	8-89
Trace: System Command Primitives	8-91
trace_grp_list	8-91
trace_grp_start	8-91
trace_id_list	8-91
trace_id_start	8-91
trace_log_trans	8-92
trace_rpt_all	8-92
trace_rpt_id	8-92
trace_stop	8-93
Trace: User Process Command Primitives	8-94
trace_appletk_parm_list	8-94
trace_appletk_start	8-94
trace_appletk_stop	8-94
trace_appn_parm_list	8-94
trace_appn_set_flags	8-95
trace_appn_stop	8-95
trace_ipproto_parm_list	8-95
trace_ipproto_start	8-95
trace_ipproto_stop	8-96
trace_snmp_list	8-96
trace_snmp_start	8-96
trace_snmp_stop	8-96
trace_sys_man_trans	8-97
User: System Command Primitives	8-98
user_add	8-98
user_del	8-98
user_list	8-98
user_passwd	8-99
3-Digit Display Command Primitive	8-100
read_3digit	8-100

Introduction

The fast-path environment is a command line interface that enables you to execute most of the same functions provided in the System Manager screens. The fast-path command environment uses command primitives to execute IBM 6611 functions without having to navigate through the System Manager screens to perform the tasks.

Note: The command primitives **do not** perform error checking on all the entered parameters. Only a small number of the primitives check for valid parameter values.

The command primitives can be used in the fast-path environment, with the **rexec** command, or in **rsh** scripts.

Executing the Command Primitives

There are three ways to execute the command primitives:

- Fast-path environment
- Remote shell (**rsh**)

For more information about the **rsh** command, see "Using Remote Shell" on page 9-14.

- Remote execution (**rexec**)

For more information about the **rexec** command, see "Using Remote Execution" on page 9-13.

You can execute all of these command primitives from the fast-path environment. You can execute most of them in the RSH and REXEC environment. The command primitive explanation states the environments in which the command primitive is supported.

Most of the command primitives send their output to the screen. However, some send it directly to the transfer directory. The command primitive explanation states the file name that contains the output. There are also trace logs that run continuously and are gathered in the transfer directory.

To view any file in the transfer directory, use the **files_view_trans** primitive. When files are viewed from the fast-path environment that are longer than one screen, the More Facility is invoked.

The More Facility displays continuous text one screen at a time. It pauses after each screen and places the word *More* at the bottom of the screen followed by the percentage of the file which the more command has read. The following commands help you to use this facility:

Function	User Action
Page down	Press the space bar
Page up	Press b

Scroll one line	Press the carriage return
Search for a string	<i>/string</i>
Display current line number	Press =
Exit the facility	Press q

Note: The command primitives **do not** perform error checking on all the entered parameters. Only a small number of the primitives check for valid parameter values.

The System Manager prevents you from entering invalid values for most function parameters by forcing you to choose the values from selection lists. The parameters for the command primitives are not selected from lists. They are typed on the command line. Only a few of the parameters are checked for correct input.

There are several command primitives that list the parameter values that are valid for other command primitives. However, you have to type in the valid value, when executing the primitive. The command primitive parameter description states when a list can be used to provide valid values for the primitive.

For example, to issue a dump for a particular user process, use the **dump_process** primitive. This primitive has a parameter called *processID*. The list of all valid process IDs can be viewed by issuing the **proc_list**. To execute this function:

1. Run the **proc_list** primitive.
2. Note the process ID of the process you want to dump.
3. Run **dump_process processID**, where processID is obtained from the **proc_list** output.

Accessing the Fast-Path Environment

There are two ways that you can access the fast-path environment using the System Manager:

- Press **F3** from the System Manager main menu.
 - Type **exit** or **quit** to return to the System Manager.
- Press **Ctrl + C** from any System Manager screen.
 - If you type **exit** or **quit**, you will be logged off. There is no way to return to the System Manager.

Exiting the Fast-Path Environment

To exit the fast-path environment, type one of the following command primitives:

```
exit
quit
```

See “Fast-Path Environment Exit Commands” on page 8-53 for more information about these command primitives.

Getting Help in the Fast-Path Environment

You can get help with the command primitives by one of three methods:

1. Type **help** without specifying a primitive name. This method provides:
 - An overview for using the command primitives, including a description of the More Facility used to view the primitive output.
 - A table of the functional grouping for the primitives along with the keywords that can be used to obtain help specific for that functional grouping.
 - A table of all primitive names in alphabetical order.
2. Another method is to type **help** along with a group prefix. This method provides help for the commands in that group. Table 8-1 lists the group prefixes that access help information.
3. The last method is to type **help** followed by the full primitive name. This method returns help for the requested command primitive.

Table 8-1 (Page 1 of 2). Group Prefixes for Accessing Help in the Fast-Path Environment

Primitive Headings	Group Prefixes
"Adapter Debug Facility Command Primitives" on page 8-10	adp, adapter, or adp_debug
"Address Resolution Protocol: Adapter Command Primitives" on page 8-12	arp or arp_adp
"Address Resolution Protocol: System Command Primitives" on page 8-16	arp or arp_sys
"Bridging Debug Facility Command Primitives" on page 8-19	brdg, bridge, bridging, or brdg_debug
"Configuration Command Primitives" on page 8-25	config or configuration
"DECnet Debug Facility Command Primitives" on page 8-29	dec, DECnet, decnet, or dec_debug
"Diskette Command Primitives" on page 8-37	disk or diskette
"Dump: System Command Primitives" on page 8-40	dump or sys_dump
"Dump: User Process Command Primitives" on page 8-42	dump or user_dump
"Error Report Command Primitives" on page 8-43	err, error, or error
"Fast-Path Environment Exit Commands" on page 8-53	exit or quit
"File Management Command Primitives" on page 8-54	file or files
"Hardware Command Primitives" on page 8-57	hw, hard, or hardware
"Host Name Command Primitives" on page 8-60	host or host_name
"Host Name to IP Address Mapping Command Primitives" on page 8-61	map, host_map, host_mapping
"Install Command Primitives" on page 8-62	install, sw

Table 8-1 (Page 2 of 2). Group Prefixes for Accessing Help in the Fast-Path Environment

Primitive Headings	Group Prefixes
"Name Server Command Primitives" on page 8-66	name or name_serv
"Process Command Primitives" on page 8-68	proc or process
"Remote Access Commands" on page 8-70	remote or commands
"Route Table Command Primitives" on page 8-73	route or route_table
"Serial Port Command Primitives" on page 8-74	serial, s1, s2, or modem
"Shutdown: System Command Primitives" on page 8-76	shut, shutdown, or sys_shutdown
"Software Lock Primitive" on page 8-78	sw
"Software VPD Command Primitives" on page 8-79	sw, soft, software, or swvpd
"Statistic-Gathering Command Primitives" on page 8-81	stat, statistic, or statistics
"Terminal Control Primitives" on page 8-86	terminal, term
"Time Server Command Primitives" on page 8-87	time or time_serv
"Time: System Command Primitives" on page 8-89	time or sys_time
"Trace: System Command Primitives" on page 8-91	trc, trace, or sys_trace
"Trace: User Process Command Primitives" on page 8-94	trc, trace, or user_trace
"User: System Command Primitives" on page 8-98	user
"3-Digit Display Command Primitive" on page 8-100	read or 3digit

Adapter Debug Facility Command Primitives

adp_dump

Function: Dumps the specified peer-capable adapter memory.

Parameters:

- adapter name
Use adp_name_list.

System Manager Equivalent: Dump Adapter Memory

Results: The adapter dump is sent to the transfer directory as:

- pd_adapter.dram
- pd_adapter.sram
- pd_adapter.prom
- pd_adapter.regs

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

adp_line_trc_start

Function: Starts a line trace on a specified peer-capable adapter.

Parameters:

1. adapter name
Use adp_name_list.
2. *n packets*
The trace stops when *n packets* are traced.

System Manager Equivalent: Start Adapter Line Trace

Results: The line trace is started.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

adp_name_list

Function: List the peer-capable adapter names.

Parameters: None

System Manager Equivalent: Use Adapter Debug Facility pop-up list.

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

adp_read_mem

Function: Read the specified peer-capable adapter memory starting at the specified address for the specified number of words.

Parameters:

1. adapter name
Use adp_name_list.
2. address or symbol (in hexadecimal, to start read)
3. length (in words, four bytes)

System Manager Equivalent: Read Adapter Memory

Results: The output is displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

adp_show_regs

Function: Displays the specified peer-capable adapter registers.

Parameters:

- adapter name
Use adp_name_list.

System Manager Equivalent: View Adapter Registers

Results: The output is displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

Address Resolution Protocol: Adapter Command Primitives

arp_adp_list

Function: List all the AppleTalk ARP (AARP) table entries.

Parameters: None

System Manager Equivalent: View Adapter AARP Entries

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

arp_adp_add_perm_nopub

Function: Add a permanent ARP table entry to a specified peer-capable adapter and do not publish it.

Parameters:

1. host name (or IP address)

The host's IP address can be used in place of the host name, if not known.

2. hardware address
3. interface name

Use interface_list, only the te# and tk# interfaces are valid.

System Manager Equivalent: Add Adapter ARP Entry

Results: The entry is added to the peer-capable adapter ARP table.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

arp_adp_add_perm_pub

Function: Add a permanent ARP table entry to a specified peer-capable adapter and publish it.

Parameters:

1. host name (or IP address)

The host's IP address can be used in place of the host name, if not known.

2. hardware address
3. interface name

Use interface_list, only the te# and tk# interfaces are valid.

System Manager Equivalent: Add Adapter ARP Entry

Results: The entry is added to the peer-capable adapter ARP table.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

arp_adp_add_temp_nopub

Function: Add a temporary ARP table entry to a specified peer-capable adapter and do not publish it.

Parameters:

1. host name (or IP address)

The host's IP address can be used in place of the host name, if not known.

2. hardware address

3. interface name

Use interface_list, only the te# and tk# interfaces are valid.

System Manager Equivalent: Add Adapter ARP Entry

Results: The entry is added to the peer-capable adapter ARP table.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

arp_adp_add_temp_pub

Function: Add a temporary ARP table entry to a specified peer-capable adapter and publish it.

Parameters:

1. host name (or IP address)

The host's IP address can be used in place of the host name, if not known.

2. hardware address

3. interface name

Use interface_list, only the te# and tk# interfaces are valid.

System Manager Equivalent: Add a temporary adapter ARP table entry and publish it. Add Adapter ARP Entry

Results: The entry is added to the peer-capable adapter ARP table.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

arp_adp_del_addr

Function: Delete an ARP table entry from a specified peer-capable adapter indexed by hardware address.

Parameters:

1. hardware address

2. interface name

Use interface_list, only the te# and tk# interfaces are valid.

Address Resolution Protocol: Adapter Command Primitives

System Manager Equivalent: Delete Adapter ARP Entry With Hardware Address

Results: The entry is deleted from the peer-capable adapter ARP table.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

arp_adp_del_host

Function: Delete an ARP table entry for a specified peer-capable adapter indexed by host name.

Parameters:

1. host name (IP address)
The host's IP address can be used in place of the host name, if not known.
2. interface name
Use interface_list, only the te# and tk# interfaces are valid.

System Manager Equivalent: Delete Adapter ARP Entry With Host Name

Results: The entry is deleted from the adapter ARP table.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

arp_adp_flush

Function: Delete all ARP table entries for the specified peer-capable adapter.

Parameters:

- interface name
Use interface_list, only the te# and tk# interfaces are valid.

System Manager Equivalent: Clear Adapter ARP Table

Results: The ARP table for a specified peer-capable adapter is cleared.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

arp_adp_list

Function: List all the ARP table entries for the specified adapter.

Parameters:

- interface name
Use interface_list, only the te# and tk# interfaces are valid.

System Manager Equivalent: View Adapter ARP Entries

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

interface_list

Function: List the names of the available adapter interfaces.

Parameters: None

System Manager Equivalent: Interface name selector that occurs with many System Manager functions.

Results: The output is displayed on the terminal. Only the adapter interfaces for the token-ring and Ethernet peer-capable adapters are valid for the adapter ARP table primitives.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

Address Resolution Protocol: System Command Primitives

arp_hw_type_list

Function: List the supported hardware types.

Parameters: None

System Manager Equivalent: Add Adapter ARP Entry hardware type pop-up list

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

arp_sys_add_perm_nopub

Function: Add a permanent system ARP table entry and do not publish it.

Parameters:

1. hardware type
Use arp_hw_type_list.
2. host name (or IP address)
The host's IP address can be used in place of the host name, if not known.
3. hardware address

System Manager Equivalent: Add System ARP Entry

Results: The entry is added to the system ARP table.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

arp_sys_add_perm_pub

Function: Add a permanent system ARP table entry and publish it.

Parameters:

1. hardware type
Use arp_hw_type_list.
2. host name (or IP address)
The host's IP address can be used in place of the host name, if not known.
3. hardware address

System Manager Equivalent: Add System ARP Entry

Results: The entry is added to the system ARP table.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

arp_sys_add_temp_nopub

Function: Add a temporary system ARP table entry and do not publish it.

Parameters:

1. hardware type

Use arp_hw_type_list.

2. host name (or IP address)

The host's IP address can be used in place of the host name, if not known.

3. hardware address

System Manager Equivalent: Add System ARP Entry

Results: The entry is added to the system ARP table.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

arp_sys_add_temp_pub

Function: Add a temporary system ARP table entry and publish it.

Parameters:

1. hardware type

Use arp_hw_type_list.

2. host name (or IP address)

The host's IP address can be used in place of the host name, if not known.

3. hardware address

System Manager Equivalent: Add System ARP Entry

Results: The entry is added to the system ARP table.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

arp_sys_del_host

Function: Delete a system ARP table entry indexed by host name.

Parameters:

- host name (or IP address)

The host's IP address can be used in place of the host name, if not known.

System Manager Equivalent: Delete System ARP Entry

Results: The entry is deleted from the system ARP table.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

arp_sys_list

Function: List all the system ARP table entries.

Parameters: None

System Manager Equivalent: View System ARP Entries

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

Bridging Debug Facility Command Primitives

brdg_cfg_info

Function: View the source route bridging configuration information for the specified interface.

Parameters:

- interface name

Use interface_list, only the tk# and to# interfaces are valid.

System Manager Equivalent: View Bridge Configuration Information

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

brdg_sap_filter

Function: View the source route bridging SAP filter information for the specified interface.

Parameters:

- interface name

Use interface_list, only the tk# and to# interfaces are valid.

System Manager Equivalent: View Bridge SAP Filter Information

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

port_list

Function: List the port index of the specified 2-Port Serial adapter that is configured for bridging and frame relay.

Parameters:

- interface_list

System Manager Equivalent: Source Route Bridge Spanning Tree Statistics pop-up list

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

stat_adp_brdg

Function: Display the source route bridge adapter statistics.

Parameters:

1. interface name
Use interface_list, only the tk# and to# interfaces are valid.
2. *n* seconds

System Manager Equivalent: Bridge Statistics

Results: The output is displayed on the terminal. Press Ctrl + C to end the command.

Authorization: Controlling and viewing users

System Environment: Fast path only

stat_adp_lanbr

Function: Display the adapter LAN bridge statistics.

Parameters:

1. interface name
Use interface_list, only to# interfaces are valid.
2. *n* seconds

System Manager Equivalent: LAN Bridge Statistics under View Adapter Interface Statistics

Results: The output is displayed on the terminal. Press Ctrl + C to end the command.

Authorization: Controlling and viewing users

System Environment: Fast path only

stat_srb_sptree

Function: Display the source route bridging spanning tree statistics for the specified interface every *n* seconds.

Parameters:

1. interface name
Use interface_list, only tk# and to# interfaces are valid.
2. *n* seconds

System Manager Equivalent: Source Route Bridge Spanning Tree Statistics

Results: The output is displayed on the terminal. Press Ctrl + C to end the command.

Authorization: Controlling and viewing users

System Environment: Fast path only

stat_srb_sptree_frm

Function: Display the source route bridging spanning tree frame relay statistics for the specified interface every *n* seconds.

Parameters:

1. interface name
Use interface_list, only to# interfaces are valid.
2. *n* seconds

System Manager Equivalent: Source Route Bridge Spanning Tree Frame Relay Statistics

Results: The output is displayed on the terminal. Press Ctrl + C to end the command.

Authorization: Controlling and viewing users

System Environment: Fast path only

stat_sys_lanbr

Function: Display the LAN bridge statistics for the specified interface every *n* seconds as viewed from the main operating system.

Parameters:

1. interface name
Use interface_list, only to# interfaces are valid.
2. *n* seconds

System Manager Equivalent: LAN Bridge Statistics under View System Network Statistics

Results: The output is displayed on the terminal. Press Ctrl + C to end the command.

Authorization: Controlling and viewing users

System Environment: Fast path only

stat_sys_lanbr_frm

Function: Display the internal frames for the LAN bridge protocol for the specified interface every *n* seconds.

Parameters:

1. interface name
Use interface_list, only to# interfaces are valid.
2. *n* seconds

System Manager Equivalent: LAN Bridge Internal Protocol Frame Statistics

Results: The output is displayed on the terminal. Press Ctrl + C to end the command.

Authorization: Controlling and viewing users

System Environment: Fast path only

stat_tb_sptree

Function: Display the transparent bridge spanning tree statistics for the specified interface every n seconds.

Parameters:

1. interface name

Use interface_list, only the te# and to# interfaces are valid.

2. n seconds

System Manager Equivalent: Source Route Bridge Spanning Tree Statistics

Results: The output is displayed on the terminal. Press Ctrl + C to end the command.

Authorization: Controlling and viewing users

System Environment: Fast path only

stat_tb_sptree_frm

Function: Display the transparent bridge spanning tree frame relay statistics for the specified interface every n seconds.

Parameters:

1. port

Use port_list, only to# interfaces are valid.

2. n seconds

System Manager Equivalent: Source Route Bridge Spanning Tree Frame Relay Statistics

Results: The output is displayed on the terminal. Press Ctrl + C to end the command.

Authorization: Controlling and viewing users

System Environment: Fast path only

trace_brdg_start

Function: Start the source route bridging frame trace on the specified interface.

You can trace from 1 to 32 frames. The n frames parameter can be any number from 1 to 800. If a number 32 or less is specified, that number of frames are captured and the trace is stopped. If a number greater than 32 is specified, the last 32 frames are captured.

Parameters:

1. type of frame is either:
 - t** transmitted frames
 - r** received frames
 - b** both

2. *n* frames

3. interface name

Use interface_list, only tk# and to# interfaces are valid.

System Manager Equivalent: Start Bridging Frame Trace

Results: The bridge frame trace is started.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

trace_brdg_stop

Function: Stop the source route bridging frame trace for the specified type of frame.

Parameters:

1. type of frame is either:
 - t** transmitted frames
 - r** received frames
 - b** both

2. interface name

Use interface_list, only tk# and to# interfaces are valid.

System Manager Equivalent: Stop Bridging Frame Trace

Results: The bridge frame trace is stopped.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

trace_brdg_view

Function: View the source route bridging frame trace output from the specified interface.

Parameters:

1. type of frame is either:

- t** transmitted frames
- r** received frames
- b** both

2. interface name

Use interface_list, only tk# and to# interfaces are valid.

System Manager Equivalent: View Bridging Frame Trace Output

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

Configuration Command Primitives

config_app

Function: Apply the configuration changes updated from the System Manager that were made using this userid. The applied changes can later be rejected.

Parameters: None

System Manager Equivalent: Apply Changes to Configuration Database

Results: The new configuration changes are made a part of the running configuration.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

config_com

Function: Commit the configuration changes updated from the System Manager that were made using this userid. Specify whether you want to commit only the applied configuration changes or both the applied and unapplied changes. The committed configuration changes cannot be rejected.

Parameters:

- configuration level (applied or unapplied)
 - If you choose the **applied** parameter, only the applied changes are committed.
 - If you choose the **unapplied** parameter, both the applied and unapplied changes are committed

System Manager Equivalent: Commit Changes to Configuration Database

Results: The new configuration changes are made a permanent part of the running configuration.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

config_err_rpt

Function: Generate an error report for configuration errors.

Parameters: None

System Manager Equivalent: View Configuration Error Messages

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as config.errmsgs.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

Configuration Command Primitives

config_file_run

Function: Run binary configuration file in transfer directory.

Parameters:

- configuration file name

System Manager Equivalent: Import Binary Configuration File

Results: The specified binary configuration file is made the new configuration.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

config_list

Function: List the saved configuration files. There may be up to ten configuration files saved.

Parameters: None

System Manager Equivalent: Reinstate a Saved Configuration selector list.

Results: The output is displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

config_reinstate

Function: Reinstate a saved configuration file.

Parameters

- configuration file number

Use config_list to view the list of saved configurations. State the number of the configuration file.

System Manager Equivalent: Reinstate a Saved Configuration

Results: Prior to the reinstating, System Manager rejects any unapplied configuration changes from this userid, and commits any applied configuration changes from this userid. The given configuration is restored as the current configuration. The restored configuration is given a new name that is displayed at the terminal. It reflects the time and date at which the restoration occurred. The restored configuration is automatically committed.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

config_rej

Function: Reject the configuration changes updated from the System Manager that were made using this userid. Specify whether you want to reject only the unapplied configuration changes or both the applied and unapplied changes.

Parameters:

- configuration level (applied or unapplied)
 - If you choose the applied parameter, all unapplied and applied configuration changes made by this user are rejected. The running configuration is restored to the last committed state.
 - If you choose the unapplied parameter, only unapplied configuration changes made by this user are rejected. The running configuration is not affected.

System Manager Equivalent: Reject Uncommitted Changes to Configuration Database

Results: The chosen configuration changes are rejected and the saved values are restored.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

config_rpt

Function: Generate a configuration report.

Parameters:

- report type (detailed or brief)

System Manager Equivalent: View Configuration Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as config.report.detailed or config.report.brief.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

config_script

Function: Generate a configuration script.

Parameters: None

System Manager Equivalent: View Configuration Script

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as config.script.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

config_sysid

Function: Display the following system configuration information:

- Host name
- IBM 6611 model number
- Serial number
- Configuration name
- Configuration status.

Parameters: None

System Manager Equivalent: System Manager SYSID key (F4)

Results: The output goes to the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

DECnet Debug Facility Command Primitives

dec_adj

Function: Display the DECnet adjacency vector from the *start entry* for *n* entries.

Parameters:

1. *start entry*
2. *n entries*

The *start entry* parameter must be between 1 and 1023.

The *n entries* parameter must be between 1 and 400.

The default for *start entry* is 1 and *n entries* is 400.

System Manager Equivalent: View Routing Data Structures

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

dec_area_cost

Function: Display the DECnet area cost matrix from the *start entry* for *n* entries.

Parameters:

1. *start entry*
2. *n entries*

The *start entry* parameter must be between 1 and the maximum number of areas that defaults to 63.

The *n entries* parameter must be between 1 and the maximum number of areas that defaults to 63.

The default for *start entry* is 1 and *n entries* is the maximum number of areas that defaults to 63.

System Manager Equivalent: View Routing Data Structures

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

dec_area_hop

Function: Display the DECnet area hop matrix from the *start entry* for *n* entries.

Parameters:

1. *start entry*
2. *n* entries

The *start entry* parameter must be between 1 and the maximum number of areas that defaults to 63.

The *n entries* parameter must be between 1 and the maximum number of areas that defaults to 63.

The default for *start entry* is 1 and *n entries* is the maximum number of areas that defaults to 63.

System Manager Equivalent: View Routing Data Structures

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

dec_area_min_cost

Function: Display the DECnet area minimum cost vector from the *start entry* for *n* entries.

Parameters:

1. *start entry*
2. *n* entries

The *start entry* parameter must be between 1 and the maximum number of areas that defaults to 63.

The *n entries* parameter must be between 1 and the maximum number of areas that defaults to 63.

The default for *start entry* is 1 and *n entries* is the maximum number of areas that defaults to 63.

System Manager Equivalent: View Routing Data Structures

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

dec_area_min_hop

Function: Display the DECnet area minimum cost vector from the *start entry* for *n* entries.

Parameters:

1. *start entry*
2. *n* entries

The *start entry* parameter must be between 1 and the maximum number of areas that defaults to 63.

The *n entries* parameter must be between 1 and the maximum number of areas that defaults to 63.

The default for *start entry* is 1 and *n entries* is the maximum number of areas that defaults to 63.

System Manager Equivalent: View Routing Data Structures

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

dec_area_out_adj

Function: Display the DECnet area output adjacency vector from the *start entry* for *n* entries.

Parameters:

1. *start entry*
2. *n* entries

The *start entry* parameter must be between 1 and the maximum number of areas that defaults to 63.

The *n entries* parameter must be between 1 and the maximum number of areas that defaults to 63.

The default for *start entry* is 1 and *n entries* is the maximum number of areas that defaults to 63.

System Manager Equivalent: View Routing Data Structures

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

dec_area_reach

Function: Display the DECnet area reach vector from the *start entry* for *n* entries.

Parameters:

1. *start entry*
2. *n* entries

The *start entry* parameter must be between 1 and the maximum number of areas that defaults to 63.

The *n entries* parameter must be between 1 and the maximum number of areas that defaults to 63.

The default for *start entry* is 1 and *n entries* is the maximum number of areas that defaults to 63.

System Manager Equivalent: View Routing Data Structures

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

dec_circuit

Function: Display the DECnet circuit vector from the *start entry* for *n* entries.

Parameters:

1. *start entry*
2. *n* entries

The *start entry* parameter must be between 1 and the number of circuits.

The *n entries* parameter must be between 1 and the number of circuits.

The default for *start entry* is 1 and *n entries* is the number of circuits. The maximum number of circuits in an IBM 6611 Model 170 is 14 and in an IBM 6611 Model 140 is 8.

System Manager Equivalent: View Routing Data Structures

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

dec_cost

Function: Display the DECnet cost matrix from the *start entry* for *n* entries.

Parameters:

1. *start entry*
2. *n* entries

The *start entry* parameter must be between 1 and 1023.

The *n entries* parameter must be between 1 and 400.

The default for *start entry* is 1 and *n entries* is 400.

System Manager Equivalent: View Routing Data Structures

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

dec_executor

Function: Display the DECnet executor data structure.

Parameters: None

System Manager Equivalent: View Routing Data Structures

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

dec_hop

Function: Display the DECnet hop matrix from the *start entry* for *n* entries.

Parameters:

1. *start entry*
2. *n* entries

The *start entry* parameter must be between 1 and 1023.

The *n entries* parameter must be between 1 and 400.

The default for *start entry* is 1 and *n entries* is 400.

System Manager Equivalent: View Routing Data Structures

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

dec_min_cost

Function: Display the DECnet minimum cost vector from the *start entry* for *n* entries.

Parameters:

1. *start entry*
2. *n* entries

The *start entry* parameter must be between 1 and 1023.

The *n entries* parameter must be between 1 and 1023.

The default for *start entry* is 1 and *n entries* is 1023.

System Manager Equivalent: View Routing Data Structures

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

dec_min_hop

Function: Display the DECnet minimum hop vector from the *start entry* for *n* entries.

Parameters:

1. *start entry*
2. *n* entries

The *start entry* parameter must be between 1 and 1023.

The *n entries* parameter must be between 1 and 1023.

The default for *start entry* is 1 and *n entries* is 1023.

System Manager Equivalent: View Routing Data Structures

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

dec_out_adj

Function: Display the DECnet output adjacency vector from the *start entry* for *n* entries.

Parameters:

1. *start entry*
2. *n* entries

The *start entry* parameter must be between 1 and 1023.

The *n entries* parameter must be between 1 and 1023.

The default for *start entry* is 1 and *n entries* is 1023.

System Manager Equivalent: View Routing Data Structures

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

dec_reach

Function: Display the DECnet reach vector from the *start entry* for *n* entries.

Parameters:

1. *start entry*
2. *n entries*

The *start entry* parameter must be between 1 and 1023.

The *n entries* parameter must be between 1 and 1023.

The default for *start entry* is 1 and *n entries* is 1023.

System Manager Equivalent: View Routing Data Structures

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

trace_dec_level

Function: Set the debug level of DECnet tracing to a number between 0 and 15.

Parameters:

- *debug level*

A tracing level of 0 traces only error conditions. Everything is traced with a debug level of 15.

System Manager Equivalent: Set DECnet Trace Output

Results: The debug level for the trace is set to the value that you specified.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

trace_dec_log

Function: Set the DECnet trace output destination to either the system monitor log, or to the DECnet only log. The change does not take affect until after the DECnet routing process is restarted.

Parameters:

- Destination is either:
decnet DECnet only log
system system monitor log

System Manager Equivalent: Set DECnet Trace Output

Results: The trace output is sent to the log that you specified after the system is restarted.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

trace_dec_mask

Function: Set the DECnet trace mask.

Parameters:

- *data mask*

The *data_mask* is a 32 bit number that is specified in hexadecimal with each bit corresponding to a particular action to trace. If the bit is on and the debug level of the action is less than or equal to the current debug level, the action is traced.

System Manager Equivalent: Set DECnet Trace Output

Results: The DECnet trace mask is set to the value that you specified.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

trace_dec_time

Function: Set the DECnet trace time stamp mask.

Parameters:

- *time stamp mask*

The time stamp mask is a 32 bit number that is specified in hexadecimal with each bit corresponding to a particular type of data to trace. If the bit is on, a time stamp is recorded with the data when it is traced.

System Manager Equivalent: Set DECnet Trace Output

Results: The DECnet trace time stamp mask is set to the value specified.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

Diskette Command Primitives

disk_dwn_files_dos

Function: Export a file to a DOS diskette.

Parameters:

1. system directory where file exists (transfer or static)
2. file name in system directory
Use files_list_trans or files_list_static.
3. *file name* on DOS diskette

System Manager Equivalent: Export Files to DOS Diskette

Results: The file is placed on diskette as *file name*.

Authorization: Controlling and viewing users

System Environment: Fast path only

disk_dwn_files_unix

Function: Export files to a UNIX diskette.

Parameters:

1. system directory where file exists (transfer or static)
2. archive type (append or create)
3. *file name* in system directory
Use files_list_trans or files_list_static.

System Manager Equivalent: Export Files to UNIX Diskette

Results: The file is placed on diskette *file name*.

Authorization: Controlling and viewing users

System Environment: Fast path only

disk_format_dos_hi

Function: Format a diskette at high density in the DOS format.

Parameters: None

System Manager Equivalent: Format DOS Diskette

Results: The diskette is formatted.

Authorization: Controlling and viewing users

System Environment: Fast path only

disk_format_dos_low

Function: Format a diskette at low density in the DOS format.

Parameters: None

System Manager Equivalent: Format DOS Diskette

Results: The diskette is formatted.

Authorization: Controlling and viewing users

System Environment: Fast path only

disk_format_unix_hi

Function: Format a diskette at high density in the UNIX format.

Parameters: None

System Manager Equivalent: Format UNIX Diskette

Results: The diskette is formatted.

Authorization: Controlling and viewing users

System Environment: Fast path only

disk_format_unix_low

Function: Format a diskette at low density in the UNIX format.

Parameters: None

System Manager Equivalent: Format UNIX Diskette

Results: The diskette is formatted.

Authorization: Controlling and viewing users

System Environment: Fast path only

disk_list_files_dos

Function: List files on a DOS diskette.

Parameters: None

System Manager Equivalent: List Files on DOS Diskette

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: Fast path only

disk_list_files_unix

Function: List files on a UNIX diskette.

Parameters: None

System Manager Equivalent: List Files on UNIX Diskette

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: Fast path only

disk_up_files_dos

Function: Import a file from a DOS diskette.

Parameters:

1. file name on DOS diskette
Use disk_list_files_dos.
2. *file name* (in transfer directory)

System Manager Equivalent: Import Files from DOS Diskette

Results: The file is placed in the transfer directory as *file name*.

Authorization: Controlling and viewing users

System Environment: Fast path only

disk_up_files_unix

Function: Import files from a UNIX diskette.

Parameters:

- *file name(s)* to be imported
Use disk_list_files_unix.
Use "all" to import all the files on the diskette.

System Manager Equivalent: Export Files to UNIX Diskette

Results: The file is placed in the transfer directory as *file name*.

Authorization: Controlling and viewing users

System Environment: Fast path only

Dump: System Command Primitives

dump_ex_err_log

Function: Extracts error log records from the system dump.

Parameters: None

System Manager Equivalent: Extract Error Log Records From System Dump

Results: The output is displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

dump_ex_trc_log

Function: Extracts trace log records from the system dump.

Parameters: None

System Manager Equivalent: Extract Trace Log Records From System Dump

Results: The output is displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

dump_prev_info

Function: Show information about the previous system dump.

Parameters: None

System Manager Equivalent: View Previous System Dump Information

Results: The output is displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

dump_system

Function: Dump the main operating system.

Note: This command does not return and the system must be restarted.

Parameters: None

System Manager Equivalent: Start System Dump

Results: The dump goes to the dump device, */dev/hd7*.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

dump_system_format

Function: Format the system dump in either the dump device or the transfer directory and place it in the transfer directory.

Parameters:

- dump location (transfer or dump_dev)

System Manager Equivalent: View a Formatted System Dump

Results: The output is not displayed on the terminal. The formatted system dump is placed in the transfer directory as pd_system.fdump.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

dump_system_trans

Function: Copy the system dump to the transfer directory.

Parameters: None

System Manager Equivalent: Copy System Dump to Diskette or Transfer Directory

Results: The output is not displayed on the terminal. The system dump is placed in the transfer directory as pd_system.dump.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

Dump: User Process Command Primitives

dump_appn

Function: Take an APPN user process memory dump.

Parameters: None

System Manager Equivalent: Start APPN User Process Memory Dump

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as pd_dump_APPN_dn.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

dump_ipproto

Function: Dump the IP routing protocols process.

Parameters: None

System Manager Equivalent: Start IP Routing Protocols Dump

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as pd_route_proto_dump.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

dump_process

Function: Take a user process memory dump.

Parameters:

- process ID
Use proc_list.

System Manager Equivalent: Start User Process Memory Dump

Results: The output is not displayed on the terminal. The dump is placed in the transfer directory as pd_dump.process.nnnn.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

proc_list

See proc_list on page 8-68.

Error Report Command Primitives

err_id_list

Function: List all the error IDs that can be found in an error report.

Parameters: None

System Manager Equivalent: View an Error Report pop-up list

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_log_trans

Function: Place a copy of the error log into the transfer directory.

Parameters: None

System Manager Equivalent: Copy Error Log or Trace Log to Transfer Directory

Results: The error log is placed in the transfer directory as pd_error.log.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_rpt_det

Function: Generate a detailed error report for all errors logged during a certain time period.

Parameters:

1. startdate (MMDDhhmmYY)
2. enddate (MMDDhhmmYY)

If a start date is specified, error records with earlier timestamps are excluded from the report.

If an end date is specified, error records with later timestamps are excluded from the report.

If no dates are specified, no error records are excluded from the report.

System Manager Equivalent: View an Error Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as pd_error.report.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_rpt_eid_det

Function: Generate a detailed error report for errors logged during a certain time period with the given error ID.

Parameters:

1. error ID
Use err_id_list.
2. startdate (MMDDhhmmYY)
3. enddate (MMDDhhmmYY)

If a start date is specified, error records with earlier timestamps are excluded from the report.

If an end date is specified, error records with later timestamps are excluded from the report.

If no dates are specified, no error records are excluded from the report.

System Manager Equivalent: View an Error Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as pd_error.report.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_rpt_eid_sum

Function: Generate a summary error report for errors logged during a certain time period with the given error ID.

Parameters:

1. error ID
Use err_id_list.
2. startdate (MMDDhhmmYY)
3. enddate (MMDDhhmmYY)

If a start date is specified, error records with earlier timestamps are excluded from the report.

If an end date is specified, error records with later timestamps are excluded from the report.

If no dates are specified, no error records are excluded from the report.

System Manager Equivalent: View an Error Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as pd_error.report.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_rpt_etype_det

Function: Generate a detailed error report for errors logged during a certain time period of the given error type.

Parameters:

1. error type (*PERM*, *TEMP*, *PERF*, *PEND*, or *UNKN*)
2. startdate (MMDDhhmmYY)
3. enddate (MMDDhhmmYY)

If a start date is specified, error records with earlier timestamps are excluded from the report.

If an end date is specified, error records with later timestamps are excluded from the report.

If no dates are specified, no error records are excluded from the report.

System Manager Equivalent: View an Error Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as *pd_error.report*.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_rpt_etype_sum

Function: Generate a summary error report for errors logged during a certain time period of the given error type.

Parameters:

1. error type (*PERM*, *TEMP*, *PERF*, *PEND*, or *UNKN*)
2. startdate (MMDDhhmmYY)
3. enddate (MMDDhhmmYY)

If a start date is specified, error records with earlier timestamps are excluded from the report.

If an end date is specified, error records with later timestamps are excluded from the report.

If no dates are specified, no error records are excluded from the report.

System Manager Equivalent: View an Error Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as *pd_error.report*.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_rpt_hw_det

Function: Generate a detailed error report for hardware errors logged during a certain time period.

Parameters:

1. startdate (MMDDhhmmYY)
2. enddate (MMDDhhmmYY)

If a start date is specified, error records with earlier timestamps are excluded from the report.

If an end date is specified, error records with later timestamps are excluded from the report.

If no dates are specified, no error records are excluded from the report.

System Manager Equivalent: View an Error Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as pd_error.report.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_rpt_hw_rsc_det

Function: Generate a detailed error report for hardware errors logged during a certain time period with the specific resource class.

Parameters:

1. resource class
Use hw_rsc_list.
2. startdate (MMDDhhmmYY)
3. enddate (MMDDhhmmYY)

If a start date is specified, error records with earlier timestamps are excluded from the report.

If an end date is specified, error records with later timestamps are excluded from the report.

If no dates are specified, no error records are excluded from the report.

System Manager Equivalent: View an Error Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as pd_error.report.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_rpt_hw_rsc_sum

Function: Generate a summary error report for hardware errors logged during a certain time period with the given resource class.

Parameters:

1. resource class
Use hw_rsc_list.
2. startdate (MMDDhhmmYY)
3. enddate (MMDDhhmmYY)

If a start date is specified, error records with earlier timestamps are excluded from the report.

If an end date is specified, error records with later timestamps are excluded from the report.

If no dates are specified, no error records are excluded from the report.

System Manager Equivalent: View an Error Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as pd_error.report.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_rpt_hw_sum

Function: Generate a summary error report for hardware errors logged during a certain time period.

Parameters:

1. startdate (MMDDhhmmYY)
2. enddate (MMDDhhmmYY)

If a start date is specified, error records with earlier timestamps are excluded from the report.

If an end date is specified, error records with later timestamps are excluded from the report.

If no dates are specified, no error records are excluded from the report.

System Manager Equivalent: View an Error Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as pd_error.report.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_rpt_op_det

Function: Generate a detailed error report for operator errors logged during a certain time period.

Parameters:

1. startdate (MMDDhhmmYY)
2. enddate (MMDDhhmmYY)

If a start date is specified, error records with earlier timestamps are excluded from the report.

If an end date is specified, error records with later timestamps are excluded from the report.

If no dates are specified, no error records are excluded from the report.

System Manager Equivalent: View an Error Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as pd_error.report.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_rpt_op_sum

Function: Generate a summary error report for operator errors logged during a certain time period.

Parameters:

1. startdate (MMDDhhmmYY)
2. enddate (MMDDhhmmYY)

If a start date is specified, error records with earlier timestamps are excluded from the report.

If an end date is specified, error records with later timestamps are excluded from the report.

If no dates are specified, no error records are excluded from the report.

System Manager Equivalent: View an Error Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as pd_error.report.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_rpt_seq

Function: Generate an error report for a given sequence number.

Parameters:

- sequence number

Use seq_num_list.

System Manager Equivalent: View an Error Report for a Single Sequence Number

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_rpt_sum

Function: Generate a summary report for all errors logged during a certain time period.

Parameters:

1. startdate (MMDDhhmmYY)
2. enddate (MMDDhhmmYY)

If a start date is specified, error records with earlier timestamps are excluded from the report.

If an end date is specified, error records with later timestamps are excluded from the report.

If no dates are specified, no error records are excluded from the report.

System Manager Equivalent: View an Error Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as pd_error.report.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_rpt_sw_det

Function: Generate a detailed error report for software errors logged during a certain time period.

Parameters:

1. startdate (MMDDhhmmYY)
2. enddate (MMDDhhmmYY)

If a start date is specified, error records with earlier timestamps are excluded from the report.

If an end date is specified, error records with later timestamps are excluded from the report.

Error Report Command Primitives

If no dates are specified, no error records are excluded from the report.

System Manager Equivalent: View an Error Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as pd_error.report.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_rpt_sw_rsc_det

Function: Generate a detailed error report for software errors logged during a certain time period with the given resource name.

Parameters:

1. resource name
Use sw_rsc_list.
2. startdate (MMDDhhmmYY)
3. enddate (MMDDhhmmYY)

If a start date is specified, error records with earlier timestamps are excluded from the report.

If an end date is specified, error records with later timestamps are excluded from the report.

If no dates are specified, no error records are excluded from the report.

System Manager Equivalent: View an Error Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as pd_error.report.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_rpt_sw_rsc_sum

Function: Generate a summary error report for software errors logged during a certain time period with the given resource name.

Parameters:

1. resource name
Use sw_rsc_list.
2. startdate (MMDDhhmmYY)
3. enddate (MMDDhhmmYY)

If a start date is specified, error records with earlier timestamps are excluded from the report.

If an end date is specified, error records with later timestamps are excluded from the report.

If no dates are specified, no error records are excluded from the report.

System Manager Equivalent: View an Error Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as `pd_error.report`.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_rpt_sw_sum

Function: Generate a summary error report for software errors logged during a certain time period.

Parameters:

1. startdate (MMDDhhmmYY)
2. enddate (MMDDhhmmYY)

If a start date is specified, error records with earlier timestamps are excluded from the report.

If an end date is specified, error records with later timestamps are excluded from the report.

If no dates are specified, no error records are excluded from the report.

System Manager Equivalent: View an Error Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as `pd_error.report`.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

err_type_list

Function: List the valid error types.

Parameters: None

System Manager Equivalent: View an Error Report pop-up list

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

hw_rsc_list

Function: List the hardware resources classes that can be found in an error report.

Parameters: None

System Manager Equivalent: View an Error Report pop-up list

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

seq_num_list

Function: List the sequence number of the error records that currently reside in the error log.

Parameters: None

System Manager Equivalent: View an Error Report for a Single Sequence Number pop-up list

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

sw_rsc_list

Function: List the software resources names that can be found in an error report.

Parameters: None

System Manager Equivalent: View an Error Report pop-up list

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

Fast-Path Environment Exit Commands

exit

Function: Issue this command to exit the fast-path environment and return to the System Manager, if the fast-path environment was entered using F3 (Esc + 3) from the main System Manager Menu. If the fast-path environment was entered using Ctrl + C, you are logged out of the IBM 6611.

Parameters: None

System Manager Equivalent: No equivalent

Results: If the fast-path environment was entered using F3 (Esc + 3) from the main System Manager Menu, you are returned to the System Manager. If the fast-path environment was entered using Ctrl + C, you are logged out of the IBM 6611.

Authorization: Controlling and viewing users

System Environment: Fast path only

quit

Function: Issue quit to exit the fast-path environment and the Multiprotocol Network Program.

Parameters: None

System Manager Equivalent: No equivalent

Results: You are logged out of the IBM 6611.

Authorization: Controlling and viewing users

System Environment: Fast path only

File Management Command Primitives

files_clr_all_trans

Function: Delete ALL the files from the transfer directory.

Warning: This is dangerous and should only be used in extreme circumstances.

Parameters: None

System Manager Equivalent: Work with Files in Transfer Directory

Results: ALL the files in the transfer directory are deleted.

Warning: Deleting ALL the files in the transfer directory may result in the loss of needed problem determination output.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

files_clr_one_trans

Function: Delete one file from the transfer directory.

Parameters:

- file name

Use files_list_trans.

System Manager Equivalent: Work with Files in Transfer Directory

Results: The specified file is deleted from the transfer directory.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

files_list_static

Function: List all files in the static directory.

Parameters: None

System Manager Equivalent: View a File in Static Directory pop-up list

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

files_list_trans

Function: List all files in the transfer directory.

Parameters: None

System Manager Equivalent: Work with Files in Transfer Directory pop-up list

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

files_rename_trans

Function: Change the name of a file in the transfer directory.

Parameters:

1. current file name
Use files_list_trans.
2. new file name

System Manager Equivalent: Work with Files in Transfer Directory

Results: The name of a file in the transfer directory is changed.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

files_view_static

Function: View a file in the static directory. Both binary and text files can be viewed.

Parameters:

- file name
Use files_list_static.

System Manager Equivalent: View a File in Static Directory

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

files_view_trans

Function: View a file in the transfer directory.

Parameters:

- file name

Use files_list_trans.

System Manager Equivalent: Work with Files in Transfer Directory

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

Hardware Command Primitives

hw_cfg_chg

Function: Update hardware VPD after configuration changes.

Parameters: None

System Manager Equivalent: Update Hardware Vital Product Data After Configuration Changes

Results: The hardware VPD is updated to reflect hardware configuration changes.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

hw_def_list

Function: List all the defined devices.

Parameters: None

System Manager Equivalent: List All Defined Devices

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

hw_detail

Function: Display the characteristics of a defined device.

Parameters:

- device name
- Use hw_def_list.

System Manager Equivalent: View Characteristics of a Defined Device

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

hw_diag

Function: Run concurrent diagnostics on a specified device.

Parameters:

- diagnostic device
- Use hw_diag_list.

System Manager Equivalent: Concurrent Hardware Diagnostics

Results: The diagnostic output is displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

hw_diag_list

Function: List devices supported with diagnostics.

Parameters: None

System Manager Equivalent: Concurrent Hardware Diagnostics list

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

hw_install_list

Function: List all the installed devices.

Parameters: None

System Manager Equivalent: List All Installed Devices

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

hw_serial_model

Function: Displays or updates the IBM 6611 serial number and model number.

Parameters: To display: None

To update:

- serial_number

Must have the format:

XX-NNNNNNN

where XX is the alphanumeric uppercase prefix and NNNNNNN is the alphanumeric suffix.

- model_number

The model number is 120, 140, or 170.

System Manager Equivalent: None

Results: The serial number and model number are displayed at the terminal or the hardware vital product data is updated.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

hw_sup_list

Function: List all supported devices.

Parameters: None

System Manager Equivalent: List All Supported Devices

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

hw_vpd_list

Function: List the hardware VPD.

Parameters: None

System Manager Equivalent: View Hardware Vital Product Data

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

Host Name Command Primitives

host_name_set

Function: Sets the host name and domain name for this IBM 6611.

Parameters:

1. host name (up to 31 characters)
2. domain name (up to 63 characters)

System Manager Equivalent: Set Host Name Information

Results: The new settings are displayed.

This configuration change must be applied or committed for it to become a part of the working configuration (config_app or config_com).

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

host_name_show

Function: Display the host name and domain name for this IBM 6611.

Parameters: None

System Manager Equivalent: Set Host Name Information

Results: The current settings for host name and domain name are displayed.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

Host Name to IP Address Mapping Command Primitives

map_host_add

Function: Add a host name and IP address pair to the mapping.

Parameters:

1. host name
2. IP address

System Manager Equivalent: Add a Host Name to the Mapping

Results: The host name and IP address pair is added to the mapping.

This configuration change must be applied or committed for it to become a part of the working configuration (config_app or config_com).

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

map_host_del

Function: Delete a host name and IP address pair from the mapping.

Parameters:

1. host name
- Use map_host_list.

System Manager Equivalent: Delete a Host Name from the Mapping

Results: The host name and IP address pair is deleted from the mapping.

This configuration change must be applied or committed for it to become a part of the working configuration (config_app or config_com).

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

map_host_list

Function: List host names and their IP addresses.

Parameters: None

System Manager Equivalent: List All Static Host Name Mappings

Results: The host names are listed with their IP addresses.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

Install Command Primitives

install_cleanup

Function: Removes all incomplete pieces of software after a failed install.

Parameters: None

System Manager Equivalent: Clean Up After a Failed Installation

Results: The install messages are displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

install_comp

Function: Install the software components in the transfer directory. Specify either a forced or normal installation and whether or not to restart the IBM 6611 after a successful installation.

Parameters:

1. installation type (force or normal)
2. restart type (restart or norestart)
3. component name (mpnp.obj or mpnp.data or mpnp.all)

System Manager Equivalent: Apply Software Components

Results: The install messages are displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

install_fix_list

Function: List the problems fixed by the software updates in the transfer directory.

Parameters:

- update name(s) or *all*
Use install_sw_list.

System Manager Equivalent: List All Problems Fixed by Software Updates in Transfer Directory

Results: The output is displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

install_not_commit_list

Function: List software that has been installed but not committed.

Parameters: None

System Manager Equivalent: List All Applied but Not Committed Software

Results: The output is displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

install_reinstate_saved_comp

Function: Reinstate saved software component. Specify whether or not to restart the IBM 6611 after a successful restoration of the saved component.

Parameters:

- restart type (restart or norestart)

System Manager Equivalent: Reinstate Saved Software Component

Results: The install messages are displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

install_remove_saved_comp

Function: Remove saved software component.

Parameters: None

System Manager Equivalent: Remove Saved Software Component

Results: The install messages are displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

install_sw_list

Function: List all software in the transfer directory.

Parameters: None

System Manager Equivalent: List All Software in the Transfer Directory

Results: The output is displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

install_up_trans

Function: Import all software from diskette to transfer directory.

Parameters: None

System Manager Equivalent: Import Software to Transfer Directory

Results: The software updates and components are placed in the transfer directory.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

install_upd

Function: Install the software updates in the transfer directory. Specify whether or not to restart the IBM 6611 after a successful installation.

Parameters:

1. restart type (restart or norestart)
2. update name(s) or *all*

Use install_sw_list.

System Manager Equivalent: Apply Software Updates

Results: The install messages are displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

install_upd_commit

Function: Commit software updates that have been applied.

Parameters:

- update name(s) or *all*

Use install_not_commit_list.

System Manager Equivalent: Commit Applied Updates (Delete Previous Version)

Results: The install messages are displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

install_upd_reject

Function: Reject software updates that have been installed, but not committed.

Parameters:

- update name(s)

Use install_not_commit_list.

System Manager Equivalent: Reject Applied Updates (Use Previous Version)

Results: The install messages are displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

install_verify

Function: Verify a software component.

Parameters:

- component name (mpnp.obj or mpnp.data)

System Manager Equivalent: Verify a Software Component

Results: The verify messages are displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

Name Server Command Primitives

name_serv_add

Function: Add a host to the list of remote host name servers.

Parameters:

- IP address

System Manager Equivalent: Add a Name Server

Results: The remote host name server is added to the list of name servers.

This configuration change must be applied or committed for it to become a part of the working configuration (config_app or config_com).

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

name_serv_del

Function: Delete a host from the list of remote host name servers.

Parameters:

- IP address

Use name_serv_list.

System Manager Equivalent: Delete a Name Server

Results: The remote host name server is deleted from the list of name servers.

This configuration change must be applied or committed for it to become a part of the working configuration (config_app or config_com).

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

name_serv_list

Function: List IP addresses of all host name servers.

Parameters: None

System Manager Equivalent: List All Name Servers

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

name_serv_start

Function: Start using remote host name service.

Parameters: None

System Manager Equivalent: Start Using Name Service

Results: The remote host name service is enabled.

This configuration change must be applied or committed for it to become a part of the working configuration (config_app or config_com).

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

name_serv_stop

Function: Stop using remote host name service.

Parameters: None

System Manager Equivalent: Stop Using Name Service

Results: The remote host name service is disabled.

This configuration change must be applied or committed for it to become a part of the working configuration (config_app or config_com).

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

Process Command Primitives

proc_command

Function: List the process commands with the full path name and all arguments.

Parameters: None

System Manager Equivalent: List Process Commands

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

proc_info

Function: List detailed information about running processes.

Parameters: None

System Manager Equivalent: View Process Information

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

proc_list

Function: List the running processes.

Parameters: None

System Manager Equivalent: List Processes

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

proc_stat

Function: Display the status of the active running processes.

Parameters: None

System Manager Equivalent: View Process Status

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

proc_table

Function: Display the process table information.

Parameters: None

System Manager Equivalent: View Process Table Information

Results: The output is displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

Remote Access Commands

atecho

Function: Issue an atecho request to test for the existence of a route to another AppleTalk address.

Parameters:

1. -c
2. *number of requests*
3. *network id*
4. *node id*

System Manager Equivalent: Issue Atecho to Any AppleTalk Node

Results: The atecho requests are sent and the responses are displayed.

Authorization: Controlling and viewing users

System Environment: Fast path only

ftp

Function: Issue FTP to send or receive a file to or from a remote IP station. This is an interactive session. You are prompted for the userid and password at the remote host. See "Using the File Transfer Protocol" on page 10-52 for details.

Parameters:

- host name (or IP address)

System Manager Equivalent: Send Files to Another Node or Receive Files from Another Node

Results: You can send or receive files from the remote host.

Authorization: Controlling and viewing users

System Environment: Fast path only

modem_rcv

Function: Receive a file using Xmodem.

Parameters:

- file name

System Manager Equivalent: Receive Files from Another Node

Results: The Xmodem messages are displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: Fast path only

modem_send

Function: Send a file from the specified directory using Xmodem.

Parameters:

1. directory name (transfer or static)
2. file name

System Manager Equivalent: Send Files to Another Node

Results: The Xmodem messages are displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: Fast path only

ping

Function: Issue a ping request to test for the existence of a route to another IP node.

Parameters:

1. host name (or IP address)
2. packet size in bytes
3. number of requests to send

System Manager Equivalent: Issue Ping to Any IP Node

Results: The ping requests are sent and the responses are displayed.

Authorization: Controlling and viewing users

System Environment: Fast path only

rlogin

Function: Issue rlogin to login to another IBM 6611. This is an interactive session. You are prompted for the password at the remote host. See "Using Remote Login" on page 9-10 for details.

Parameters:

1. host name (or IP address)
2. -8 -l userid

System Manager Equivalent: Issue Remote Login to Any IP Node

Results: You are logged into the remote host.

Authorization: Controlling and viewing users

System Environment: Fast path only

telnet

Function: Issue telnet to log in to another IP node. This is an interactive session. You are prompted for user id and password at the remote host. See “Using TELNET” on page 9-8 for details.

Parameters:

- host name (or IP address)

System Manager Equivalent: Issue Telnet to Any IP Node

Results: You are logged into the remote host.

Authorization: Controlling and viewing users

System Environment: Fast path only

Route Table Command Primitives

interface_list

See interface_list on page 8-15.

route_adp_table

Function: Display the route table on a specified peer-capable adapter for a specified protocol:

- IP
- XNS
- IPX
- DECnet
- AppleTalk.

Parameters:

1. protocol name (*inet*, *ns*, *ipx*, *decnet*, or *appletalk*)
2. interface name

Use interface_list, only the te#, tk#, and to# interfaces are valid.

System Manager Equivalent: View Adapter Route Tables

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

route_sys_table

Function: Display the system routing table.

Parameters: None

System Manager Equivalent: View System Route Table

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

Serial Port Command Primitives

modem_recv

Function: Receive a file using Xmodem.

Parameters:

- file name

System Manager Equivalent: Receive Files from Another Node

Results: The Xmodem messages are displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: Fast path only

modem_send

Function: Send a file from the specified directory using Xmodem.

Parameters:

1. directory name (transfer or static)
2. file name

System Manager Equivalent: Send Files to Another Node

Results: The Xmodem messages are displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: Fast path only

s1_at

Function: Send AT commands to a modem on the EIA 232 serial port S1 or Serial 1. Do not issue this command if you are logged in over the S1 or Serial 1 port.

Parameters:

- AT commands

System Manager Equivalent: Send AT Command to Modem on Serial Port

Results: AT commands are sent to the modem on the S1 or Serial 1 port.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

s1_baud

Function: Set baud rate on the EIA 232 serial port S1 or Serial 1. Do not issue this command if you are logged in over the S1 or Serial 1 port.

Parameters:

- baud rate (1200, 2400, 9600, 19200, 38400)

System Manager Equivalent: Configure EIA/232 Serial Ports

Results: The baud rate is set as specified.

This configuration change must be applied or committed for it to become a part of the working configuration (config_app or config_com).

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

s2_at

Function: Send AT commands to a modem on the EIA 232 serial port S2 or Serial 2. Do not issue this command if you are logged in over the S2 or Serial 2 port, or if you are using the S2 or Serial 2 port for a Cylink connection.

Parameters:

- AT command (s)

System Manager Equivalent: Send AT Command to Modem on Serial Port

Results: AT commands are sent to the modem on the S2 port.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

s2_baud

Function: Set baud rate on the EIA 232 serial port S2 or Serial 2. Do not issue this command if you are logged in over this port or if you are using this port for a Cylink connection.

Parameters:

- baud rate (1200, 2400, 9600, 19200, 38400)

System Manager Equivalent: Configure EIA/232 Serial Ports

Results: The baud rate is set as specified.

This configuration change must be applied or committed for it to become a part of the working configuration (config_app or config_com).

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

Shutdown: System Command Primitives

shutdown_at_ipl

Function: Shut down the IBM 6611 at the specified time and restart it.

Parameters:

- time (hh:mm)

System Manager Equivalent: Stop the System With or Without Re-IPL

Results: The system is shut down and restarted. You will lose your session, when the system shuts down.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

shutdown_at_noipl

Function: Shut down the IBM 6611 at the specified time and do not restart it.

Parameters:

- time (hh:mm)

System Manager Equivalent: Stop the System With or Without Re-IPL

Results: The system is shut down without a restart. You will have to restart the IBM 6611 using the Reset button.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

shutdown_soon_ipl

Function: Shut down the IBM 6611 in the number of minutes specified and restart it.

Parameters:

- *n* minutes

System Manager Equivalent: Stop the System With or Without Re-IPL

Results: The system is shut down and restarted. You will lose your session, when the system shuts down.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

shutdown_soon_noipl

Function: Shut down the IBM 6611 in the number of minutes specified and do not restart it.

Parameters:

- *n* minutes

System Manager Equivalent: Stop the System With or Without Re-IPL

Results: The system is shut down without a restart. You will have to restart the IBM 6611 using the Reset button.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

Software Lock Primitive

sw_lock

Function: Locks the Multiprotocol Network Program when selling the IBM 6611 to a third party.

Parameters: None

System Manager Equivalent: No equivalent

Results: The Multiprotocol Network Program is locked. Use a start up configuration diskette to unlock.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

Software VPD Command Primitives

sw_dep_list

Function: List the software updates dependent on the given software.

Parameters:

- software name
- Use sw_list.

System Manager Equivalent: List Dependents of a Software Component

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

sw_files_list

Function: List the files included in a software component.

Parameters:

- component name (mpnp.obj or mpnp.data)

System Manager Equivalent: List Files Included in a Software Component

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

sw_history

Function: Display the history of a software component.

Parameters:

- component name (mpnp.obj or mpnp.data)

System Manager Equivalent: View History of a Software Component

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

sw_id

Function: Displays the product information for an installed software component.

Parameters:

- component name (mpnp.obj or mpnp.data)

System Manager Equivalent: View ID of a Software Component

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

sw_list

Function: List all installed software components.

Parameters: None

System Manager Equivalent: List All Installed Software

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

sw_prereq

Function: Lists the prerequisite software for a given software update.

Parameters:

- update name
Use sw_list.

System Manager Equivalent: List Prerequisites of a Software Component

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

sw_upd_list

Function: List the software updates to a given software component.

Parameters:

- component name (mpnp.obj or mpnp.data)

System Manager Equivalent: List All Updates to a Software Component

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

Statistic-Gathering Command Primitives

interface_list

See interface_list on page 8-15.

stat_adp_con

Function: Display adapter connection statistics for the IP, IPX, XNS and DECnet protocols.

Parameters:

1. protocol name (*inet, ns, ipx, decnet*)
2. interface name

Use interface_list, only the te#, tk#, and to# interfaces are valid.

System Manager Equivalent: Connection Statistics under View Adapter Interface Statistics

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

stat_adp_filter

Function: Display the adapter filter information for the following protocols: IP, XNS, IPX, and DECnet. You must have filters configured before issuing this command.

Parameters:

1. protocol name (*inet, ns, ipx, decnet*)
2. interface name

Use interface_list, only the te#, tk#, and to# interfaces are valid.

System Manager Equivalent: Filter Information under View Adapter Interface Statistics

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

stat_adp_pack_traf

Function: Display the adapter packet traffic statistics.

Parameters:

1. interface name

Use interface_list, only the te#, tk#, and to# interfaces are valid.

2. *n* seconds

System Manager Equivalent: Packet Traffic Statistics under View Adapter Interface Statistics

Results: The output is displayed on the terminal. Press Ctrl + C to end the command.

Authorization: Controlling and viewing users

System Environment: Fast path only

stat_adp_proto

Function: Display the adapter IP, IPX, XNS and DECnet protocol statistics for a specified adapter interface.

Parameters:

1. protocol name (*inet*, *ns*, *ipx*, or *decnet*)
2. interface name

Use interface_list, only the te#, tk#, and to# interfaces are valid.

System Manager Equivalent: Protocol Statistics

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

stat_adp_proto_mon

Function: Monitor the protocol and interface packet traffic information.

Parameters:

- *n* seconds

System Manager Equivalent: View Protocol and Interface Packet Traffic Information

Results: The output is displayed on the terminal. Press Ctrl + C to end the command.

Authorization: Controlling user only

System Environment: Fast path only

stat_inet

Function: Display the active internet connection statistics.

Parameters: None

System Manager Equivalent: Active Internet Connection Information

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

stat_io

Function: Display the I/O statistics every n seconds for n samples.

Parameters:

1. n seconds
2. n samples

System Manager Equivalent: View Input/Output Statistics

Results: The output is displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

stat_mem_man

Function: Display the memory management statistics.

Parameters: None

System Manager Equivalent: Memory Management Statistics

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

stat_net_con

Function: Display the network connection statistics generated by the main operating system.

Parameters: None

System Manager Equivalent: Connection Statistics under View System Network Statistics

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

stat_route

Function: Display the system route statistics.

Parameters: None

System Manager Equivalent: TCP/IP Route Statistics

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

stat_socket

Function: Display information about the domain sockets.

Parameters: None

System Manager Equivalent: System Socket Information

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

stat_sys_activity

Function: Generate a system activity report. The statistics are gathered every n seconds for n samples.

Parameters:

1. n seconds
2. n samples

System Manager Equivalent: View System Activity Report

Results: The output is displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

stat_sys_pack_traf

Function: Display the packet traffic information for the specified interface every n seconds gathered by the main operating system.

Parameters:

1. interface name
Use interface_list, any listed interface is valid.
2. n seconds

System Manager Equivalent: Packet Traffic Statistics under View System Network Statistics

Results: The output is displayed on the terminal. Press Ctrl + C to end the command.

Authorization: Controlling and viewing users

System Environment: Fast path only

stat_sys_proto

Function: Display the TCP/IP protocol statistics gathered by the main operating system.

Parameters:

- protocol name (*ip*, *tcp*, *udp*, *tpip*, or *icmp*)

All of the above protocols are listed if this parameter is left blank.

System Manager Equivalent: TCP/IP Protocol Statistics

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

stat_virt_mem

Function: Display system virtual memory statistics every *n* seconds for *n* samples.

Parameters:

1. *n* seconds
2. *n* samples

System Manager Equivalent: View Virtual Memory Statistics

Results: The output is displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

Terminal Control Primitives

set_backspace

Function: Sets the specified key or key sequence to erase backwards one character at a time, when pressed. This is normally set to Backspace.

Parameters:

- key or key sequence

System Manager Equivalent: No equivalent

Results: The specified key performs a backspace and erase character function, when pressed.

Authorization: Controlling and viewing users

System Environment: Fast path only

set_interrupt

Function: Sets the specified key or key sequence to perform a program or process interrupt, when pressed. This is normally set to Ctrl + C.

Parameters:

- key or key sequence

System Manager Equivalent: No equivalent

Results: The specified key sequence interrupts program operation. Use this key sequence whenever a function specifies that Ctrl + C is needed to end an operation.

Authorization: Controlling and viewing users

System Environment: Fast path only

Time Server Command Primitives

time_serv_add

Function: Add a host to the list of remote time servers.

Parameters:

- IP address of remote time server

System Manager Equivalent: Add a Time Server

Results: The remote time server is added to the list of time servers.

This configuration change must be applied or committed for it to become a part of the working configuration (config_app or config_com).

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

time_serv_del

Function: Delete a host from the list of remote time servers.

Parameters:

- IP address
Use time_serv_list.

System Manager Equivalent: Delete a Time Server

Results: The remote time server is deleted from the list of time servers.

This configuration change must be applied or committed for it to become a part of the working configuration (config_app or config_com).

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

time_serv_list

Function: List all remote time servers.

Parameters: None

System Manager Equivalent: List All Time Servers

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

time_serv_start

Function: Start using remote time service.

Parameters: None

System Manager Equivalent: Start Using Time Service

Results: The remote time service is enabled.

This configuration change must be applied or committed for it to become a part of the working configuration (config_app or config_com).

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

time_serv_stop

Function: Stop using remote time service.

Parameters: None

System Manager Equivalent: Stop Using Time Service

Results: The remote time service is disabled.

This configuration change must be applied or committed for it to become a part of the working configuration (config_app or config_com).

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

Time: System Command Primitives

time_date_set

Function: Change the system time and date.

Parameters:

- date/time (YYMMDDhhmm.ss)

If no argument, the current date and time are displayed.

System Manager Equivalent: Show and Change Date and Time

Results: The date and time are changed.

If the time zone is changed from the System Manager, the fast-path environment, or the RSH environment, you are required to log out of the IBM 6611 and log back into the IBM 6611 to view the change from the System Manager or fast-path environment. If the time zone is changed from the System Manager, the fast-path environment, or the RSH environment, you are required to restart the IBM 6611 to view the change from the RSH environment.

There are a set of time zones that when set do not display, even though the time changes appropriately. These are:

- (T12-12D12) New Zealand (CUT + 12)
- (T15-9D15) Japan; Korea (CUT + 9)
- (T16-8D16) Western Australia; Taiwan (CUT + 8)
- (T17-7D17) Thailand (CUT + 7)
- (T18-6D18) Tashkent; USSR (CUT + 6)
- (T19-5D19) Pakistan (CUT + 5)
- (T21-3D21) Turkey; Saudi Arabia (CUT + 3)

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

time_zone_set

Function: Set the system time zone.

Parameters:

- time zone

If no argument, the current date, time and time zone are displayed.

System Manager Equivalent: Change Date, Time, and Time Zone

Results: The date, time and time zone are changed.

If the time zone is changed from the System Manager, the fast-path environment, or the RSH environment, you are required to log out of the IBM 6611 and log back into the IBM 6611 to view the change from the System Manager or fast-path environment. If the time zone is changed from the System Manager, the fast-path

environment, or the RSH environment, you are required restart the IBM 6611 to view the change from the RSH environment.

There are a set of time zones that when set do not display, even though the time changes appropriately. These are:

- (T12-12D12) New Zealand (CUT + 12)
- (T15-9D15) Japan; Korea (CUT + 9)
- (T16-8D16) Western Australia; Taiwan (CUT + 8)
- (T17-7D17) Thailand (CUT + 7)
- (T18-6D18) Tashkent; USSR (CUT + 6)
- (T19-5D19) Pakistan (CUT + 5)
- (T21-3D21) Turkey; Saudi Arabia (CUT + 3)

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

Trace: System Command Primitives

trace_grp_list

Function: List the system trace groups.

Parameters: None

System Manager Equivalent: Start System Trace pop-up list

Results: The output is displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

trace_grp_start

Function: Start a system trace on the specific trace ID groups.

Parameters:

- trace ID groups
- Use trace_grp_list.

System Manager Equivalent: Start System Trace

Results: The system trace is started.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

trace_id_list

Function: List the system trace IDs.

Parameters: None

System Manager Equivalent: Start System Trace pop-up list

Results: The output is displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

trace_id_start

Function: Start a system trace on the specified trace IDs.

Parameters:

- trace IDs
- Use trace_id_list.

System Manager Equivalent: Start System Trace

Trace: System Command Primitives

Results: The system trace is started.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

trace_log_trans

Function: Copy the system trace log to the transfer directory.

Parameters: None

System Manager Equivalent: Copy Error Log or Trace Log to Transfer Directory

Results: The trace log is placed in the transfer directory as pd_trace.log.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

trace_rpt_all

Function: Generate a system trace report for all trace IDs logged during a certain time period.

Parameters:

1. starttime (MMDDhhmmssYY)
2. endtime (MMDDhhmmssYY)

If only a start time is specified, trace records with earlier times are excluded from the report.

If no times are specified, no trace records are excluded from the report.

System Manager Equivalent: View System Trace Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as pd_trace.report.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

trace_rpt_id

Function: Generate a system trace report for all the specified trace IDs.

Parameters:

- trace IDs
Use trace_id_list.

System Manager Equivalent: View System Trace Report

Results: The output is not displayed on the terminal. The output is sent to the transfer directory as pd_trace.report.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

trace_stop

Function: Stop the system trace.

Parameters: None

System Manager Equivalent: Stop System Trace

Results: The system trace is stopped.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

Trace: User Process Command Primitives

trace_appletk_parm_list

Function: List the AppleTalk protocols trace parameters.

Parameters: None

System Manager Equivalent: View AppleTalk Protocol Trace dialog

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

trace_appletk_start

Function: Start the AppleTalk protocols trace.

Parameters:

- parameter list
Use trace_appletk_parm_list.

System Manager Equivalent: Start AppleTalk Protocol Trace

Results: The AppleTalk protocols trace is started.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

trace_appletk_stop

Function: Stop the AppleTalk protocols trace.

Parameters: None

System Manager Equivalent: Stop AppleTalk Protocol Trace

Results: The AppleTalk protocols trace is stopped.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

trace_appn_parm_list

Function: List the APPN protocols trace parameters.

Parameters: None

System Manager Equivalent: View APPN Trace Report dialog

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

trace_appn_set_flags

Function: Set the APPN protocol trace parameters.

Note: Use trace_grp_start or trace_id_start to begin tracing. Issue the trace_appn_stop command to stop tracing.

Parameters:

- parameter list
Use trace_appn_parm_list.

System Manager Equivalent: Start APPN Trace

Results: The APPN protocol trace is started.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

trace_appn_stop

Function: Stop the APPN protocol trace.

Parameters: None

System Manager Equivalent: Stop APPN Trace

Results: The APPN protocol trace is stopped.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

trace_ipproto_parm_list

Function: List the IP routing protocols trace parameters.

Parameters: None

System Manager Equivalent: Start IP Routing Protocols Trace dialog

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

trace_ipproto_start

Function: Start the IP routing protocols trace.

Parameters:

- parameter list
Use trace_ipproto_parm_list.

System Manager Equivalent: Start IP Routing Protocols Trace

Trace: User Process Command Primitives

Results: The IP routing protocols trace is started.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

trace_ipproto_stop

Function: Stop the IP routing protocols trace.

Parameters: None

System Manager Equivalent: Stop IP Routing Protocols Trace

Results: The IP routing protocols trace is stopped.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

trace_snmp_list

Function: List SNMP process names

Parameters: None

System Manager Equivalent: Start and Stop SNMP Trace pop-up list

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

trace_snmp_start

Function: Start SNMP trace on a specified process.

Parameters:

- SNMP process name
Use trace_snmp_list.

System Manager Equivalent: Start and Stop SNMP Trace

Results: The SNMP trace is started.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

trace_snmp_stop

Function: Stop SNMP trace on a specified process.

Parameters:

- SNMP process name
Use trace_snmp_list.

System Manager Equivalent: Start and Stop SNMP Trace

Results: The SNMP trace is stopped.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

trace_sys_man_trans

Function: Send the System Manager trace log to the transfer directory.

Parameters: None

System Manager Equivalent: No equivalent System Manager task

Results: The System Manager trace log for this user is sent to the transfer directory as sysman.trace.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

User: System Command Primitives

user_add

Function: Add a login userid, either controlling or viewing class.

Parameters:

1. userid
2. privilege class (controlling or viewing)
3. password

System Manager Equivalent: Add a User

Results: The userid is added to the system configuration.

This configuration change must be applied or committed for it to become a part of the working configuration (config_app or config_com).

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

user_del

Function: Delete a login userid.

Parameters:

- userid
- Use user_list.

System Manager Equivalent: Delete a User

Results: The userid is deleted from the system configuration.

This configuration change must be applied or committed for it to become a part of the working configuration (config_app or config_com).

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

user_list

Function: List all the userids and their privilege classes.

Parameters: None

System Manager Equivalent: List All Users

Results: The output is displayed on the terminal.

Authorization: Controlling and viewing users

System Environment: RSH, REXEC and fast path

user_passwd

Function: Change the password for a system user.

Parameters:

1. userid
 Use user_list.
2. old password
3. new password

System Manager Equivalent: Change User Password

Results: The specified userid's password is changed.

This configuration change must be applied or committed for it to become a part of the working configuration (config_app or config_com).

Authorization: Controlling user only, unless you are changing your own password.

System Environment: RSH, REXEC and fast path

3-Digit Display Command Primitive

read_3digit

Function: Read the setting of the 3-digit display on the operator's panel.

Parameters: None

System Manager Equivalent: Read Three-Digit Display on Operator Panel

Results: The output is displayed on the terminal.

Authorization: Controlling user only

System Environment: RSH, REXEC and fast path

Chapter 9. Accessing the IBM 6611

About This Chapter	9-2
Local Access Configurations	9-2
Stand-Alone IBM 6611	9-2
Direct-Attached Terminal	9-3
Transferring Files with Diskettes	9-3
Remote Access Configurations	9-4
Network-Attached Terminal	9-4
Modem-Attached Terminal	9-5
Extended Network Configurations	9-6
Accessing a Local IBM 6611	9-6
Accessing a Remote IBM 6611	9-7
Using an IP Network Connection	9-7
Using TELNET	9-8
Remote IP Station to IBM 6611	9-8
IBM 6611 to Any IP Station	9-10
Using Remote Login	9-10
Remote IP Station to IBM 6611	9-10
IBM 6611 to Any IP Station	9-11
Using RLOGIN for Extended Modem Connection	9-12
Using Remote Execution	9-13
Using Remote Shell	9-14
Remote IP Station to IBM 6611	9-14
IBM 6611 to Another IBM 6611	9-14
Comparing REXEC and RSH	9-15
Using Ping	9-15
Using Atecho for AppleTalk	9-16
Using a Modem	9-17
Accessing the IBM 6611 through the EIA 232 Serial Ports	9-19
General Setup Attributes	9-19
Communication Setup Attributes	9-20
Transferring Files with Serial Port Access	9-23
Logging In to an IBM 6611	9-23
Userids and Passwords	9-25
Controlling User Tasks	9-25

About This Chapter

This chapter describes the methods used to access the IBM 6611. The IBM 6611 can be accessed locally and remotely through either of the EIA 232 serial ports, S1 and S2 (labelled S1 and S2 on the Model 120 and Model 170, and labelled Serial 1 and Serial 2 on the Model 140).

Use of the S2 serial port is restricted to those users who do not have the S2 serial port configured to support network management of a Cylink 4201. See "Cylink Serial Number" on page 5-10 for configuration information.

Local Access Configurations

There are two local access configurations:

Stand-Alone IBM 6611

The IBM 6611 has no terminal attached and no connection to a network.

Direct-Attached Terminal

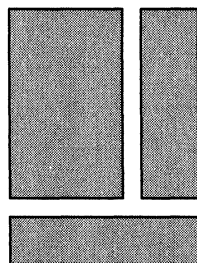
The IBM 6611 has an ASCII terminal or terminal emulator connected to one of the EIA 232 serial ports. The attached terminal must be a supported type or be able to emulate a supported type of ASCII terminal. See "Accessing the IBM 6611 through the EIA 232 Serial Ports" on page 9-19 for a list of supported ASCII terminals.

Stand-Alone IBM 6611

A minimal number of tasks can be performed from the IBM 6611 with no attached terminal. The tasks are as follows:

- Initial program load (IPL) and power off
- System dump
- Hardware diagnostics
- Replacement of failed hardware components.

To perform these tasks, you must use the operator panel controls on the front panel of the IBM 6611. This configuration is used primarily for hardware service.



IBM 6611

Figure 9-1. IBM 6611 with No Attachments

IBM service personnel service the IBM 6611 in this stand-alone configuration only under extreme circumstances when other service methods are not available. This configuration is most useful for replacing failed hardware components.

Hardware diagnostics can be run stand-alone using the set of diskettes shipped with the IBM 6611. However, the diagnostics programs are not selectable and the system is disabled while the diagnostic programs are running. Refer to the *IBM*

6611 Network Processor Installation and Service Guide (GA27-3941) for details about running stand-alone hardware diagnostics.

Note: Hardware diagnostics are run by the Customer Service Representative.

See “Start System Dump” on page 11-12 for information about system dumps. See “Starting the IBM 6611” on page 10-4 for information about an initial program load.

Direct-Attached Terminal

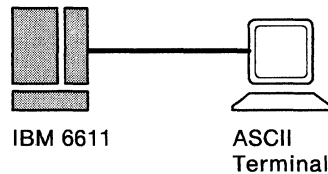


Figure 9-2. Direct-Attached Terminal

The IBM 6611 can be accessed locally by attaching an ASCII terminal or terminal emulator directly to a serial port. The attaching terminal must be a supported ASCII terminal or be able to emulate a supported ASCII terminal. See “Accessing the IBM 6611 through the EIA 232 Serial Ports” on page 9-19 for further details about the supported ASCII terminal types. See “Logging In to an IBM 6611” on page 9-23 for further details about logging in to the IBM 6611.

IBM recommends this method of accessing the IBM 6611 when the remote access configurations are not available. All operation and management tasks and most service tasks can be performed from this configuration using the System Manager or the fast-path environment.

Transferring Files with Diskettes

If remote access methods are unavailable, you can place all generated output from the System Manager or the fast-path environment on diskettes to transport to wherever needed. If you need to transport a file to the IBM 6611, such as the binary configuration file, you can also use diskettes.

If you have an IBM 6611 with less than seven peer-capable adapters, the diskette drive of the IBM 6611 is available for this function. See the following references for details about transferring files with diskettes using the diskette drive of the IBM 6611:

- “Exporting Specific Data” on page 10-50
- “Importing Specific Data” on page 10-51
- “Exporting Files to a DOS or UNIX Diskette” on page 10-25
- “Importing Files From a DOS or UNIX Diskette” on page 10-24.

If your IBM 6611 is a Model 170 with all slots occupied by peer-capable adapters, (EIA 422/449 Serial Adapter, V.35/V.36 Serial Adapter, Ethernet Adapter, and 16/4 Token-Ring Adapter), the diskette drive is disabled after the initial system start. If you have a workstation that is capable of diskette operations, you can attach it to one of the EIA 232 serial ports of the IBM 6611 and use its diskette drive. The requirements and recommended procedure for this process are explained in “Diskette Operations on a Model 170 With 7 Peer-Capable Adapters” on page 10-25.

Remote Access Configurations

Remote operations are the preferred way of servicing and managing the IBM 6611. All operation and management tasks and most service tasks can be performed remotely.

There are two remote access configurations:

Network-Attached Terminal

An ASCII or graphics terminal is connected remotely to the IBM 6611 through the IP network using remote access commands such as TELNET or RLOGIN.

Modem-Attached Terminal

The IBM 6611 has an ASCII terminal or an terminal emulator connected remotely through a modem connected to one of the EIA 232 serial ports. The attaching terminal must be a supported type or be able to emulate a supported type of ASCII terminal. See "Accessing the IBM 6611 through the EIA 232 Serial Ports" on page 9-19 for a list of supported ASCII terminals.

Network-Attached Terminal

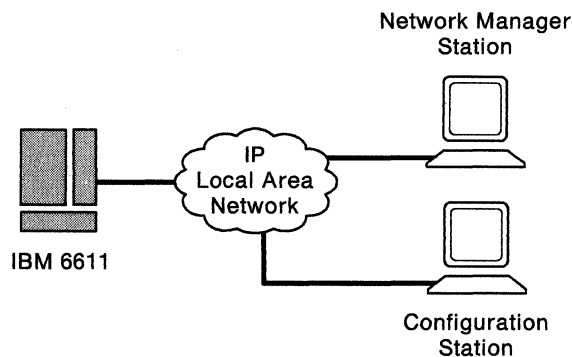


Figure 9-3. Network-Attached Terminal

The IBM 6611 has an ASCII or graphics terminal connected remotely to it through the same IP network as the IBM 6611. The remote terminal would typically be located at either the network manager station or the configuration station. This is the preferred method for accessing the IBM 6611. The supported remote access commands are:

- telnet
- rlogin
- rsh
- rexec
- ping
- atecho
- ftp.

A userid and password must be supplied when using each of these remote access commands, except for **ping** and **atecho**. When using TELNET or RLOGIN, control is passed to the System Manager after logging in and terminal verification. See "Using an IP Network Connection" on page 9-7 for details about using the remote access commands. See "Logging In to an IBM 6611" on page 9-23 for details about the login process.

Modem-Attached Terminal

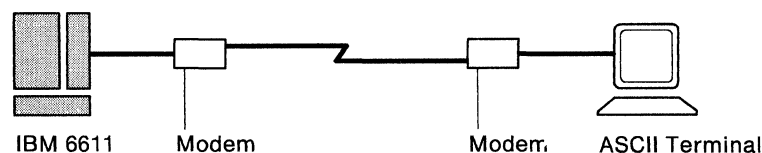


Figure 9-4. Modem-Attached Terminal

A supported ASCII terminal or any terminal that can emulate a supported ASCII terminal can attach remotely to the IBM 6611 using modems. The modem is connected to a serial port on the IBM 6611. The attaching terminal must have a communication package that can initiate the connection and must be able to support Xmodem to transfer files. See “Accessing the IBM 6611 through the EIA 232 Serial Ports” on page 9-19 for further details on the supported ASCII terminal types. See “Logging In to an IBM 6611” on page 9-23 for further details on logging into the IBM 6611.

This is the typical service configuration for the the IBM 6611. It is not necessary to have a modem attached to each of your IBM 6611s in order to use this remote service method. To access each of your IBM 6611s with remote service, only one of the IBM 6611s or another node on your IP network needs to be modem attached to use this service method. If the modem-attached node is not an IBM 6611, it must be an IP station that supports both the **rlogin** remote access command and Xmodem for transferring files.

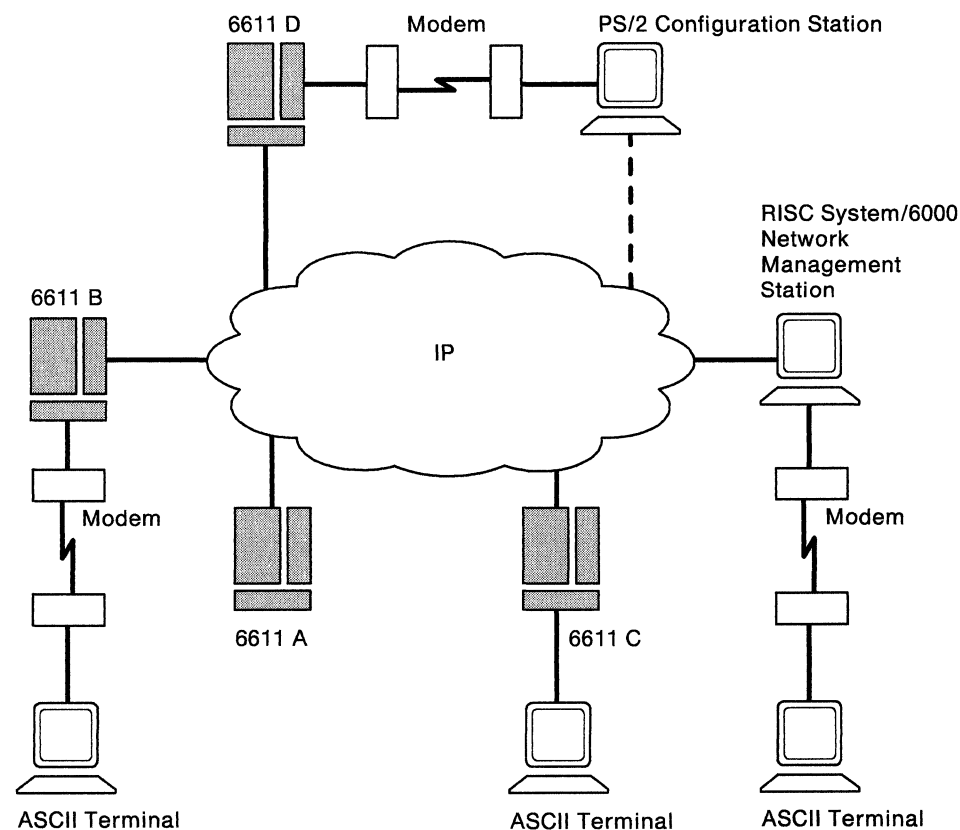


Figure 9-5. Extended Network Configuration

Extended Network Configurations

In any given IP network there are multiple possibilities for accessing the IBM 6611s. The method used at any given time depends on the particular situation and your network configuration. Figure 9-5 on page 9-5 illustrates a typical network configuration. Each of the IBM 6611s shown is attached to the IP network and can be reached using remote access commands.

IBM 6611 C has an ASCII terminal directly connected to one of its EIA 232 serial ports. This is used for service when the IP network is down or the adapter connecting the IBM 6611 to the IP network is not working. This ASCII terminal should be attached only when it is needed.

IBM 6611 B has a modem. This enables IBM service personnel to dial in and service that IBM 6611 and all IBM 6611s on the IP network. The network management station has a modem. If this station has a communication package and supports both Xmodem and RLOGIN, it can be an alternate way for the IBM service personnel to access your IBM 6611s for service. The NetView*/6000 is a network manager station that can be used in this way.

The configuration station also has a modem. If the configuration station is a PS/2 workstation, it cannot send configuration information automatically between itself and the IBM 6611. However, if the PS/2 workstation has a dial-out communication package that also supports Xmodem, a configuration file can be sent to either IBM 6611 B or the network management station to be forwarded using FTP to the IBM 6611 for which the configuration file was created. If the PS/2 has TCP/IP and supports FTP, it can use FTP to send the configuration file.

See "Accessing a Local IBM 6611" and "Accessing a Remote IBM 6611" on page 9-7 for detailed considerations and requirements for each of the access configurations.

Accessing a Local IBM 6611

Local access to the IBM 6611 is needed only in isolated situations, such as to replace hardware components or to replace remote service when there is no modem access and the IBM 6611 cannot be reached through the IP network.

Most service procedures require an ASCII terminal (or terminal emulating an ASCII device). For local access it is attached to the IBM 6611 through one of the EIA 232 serial ports. Attaching the terminal does not disrupt the operation of the IBM 6611.

When the terminal is connected to the serial port, the login screen appears. Enter a configured userid and password. After password verification, a prompt for the terminal type appears. Once the correct terminal type is entered, control is passed to the System Manager. See "Accessing the IBM 6611 through the EIA 232 Serial Ports" on page 9-19 for more information about the supported ASCII terminal types. See "Logging In to an IBM 6611" on page 9-23 for more information about logging into the IBM 6611.

Accessing a Remote IBM 6611

Remote access is the method both you and IBM service personnel use to access the IBM 6611 most of the time. All management and operation tasks can be performed over the IP network connection from your network management station. Access by modem is the best for IBM service personnel.

If IBM service personnel are given access to the IBM 6611, you do not need to know how to issue dumps and traces or retrieve problem, performance or configuration information. IBM service personnel can perform all the problem determination tasks and gather all the data they need.

Using an IP Network Connection

Using the IP network, the following IP commands can access the IBM 6611:

- TELNET (**telnet**)
- remote login (**rlogin**)
- File Transfer Protocol (**ftp**)
- remote shell (**rsh**)
- remote execution (**rexec**)
- ICMP echo (**ping**).

When you use each of these commands depends on the specific situation and location at which the command is being issued. If you are located at an IP node on your IP network that is not an IBM 6611, you can issue any of the commands listed above to your IBM 6611, provided the IP node supports the command. The same commands can also be issued from the System Manager or from the fast-path environment of any IBM 6611 to another IBM 6611. Each of the above commands, except **rsh** and **rexec**, can be issued from the System Manager or from the fast-path environment of an IBM 6611 to another node on the IP network that is not an IBM 6611.

In the sections that follow, each of the remote access commands is discussed in detail with explanations of how these commands are issued to and from an IBM 6611. There are command primitives that are used with the **rsh** and **rexec** commands. See Chapter 8 for descriptions of each of these commands.

When you use the System Manager to execute these remote access commands, there is a specific menu for all these functions that are accessed from the main menu, called the Remote Accesses to Other Nodes menu. See Figure 9-6 on page 9-8 for the functions available on the Remote Accesses to Other Nodes menu.

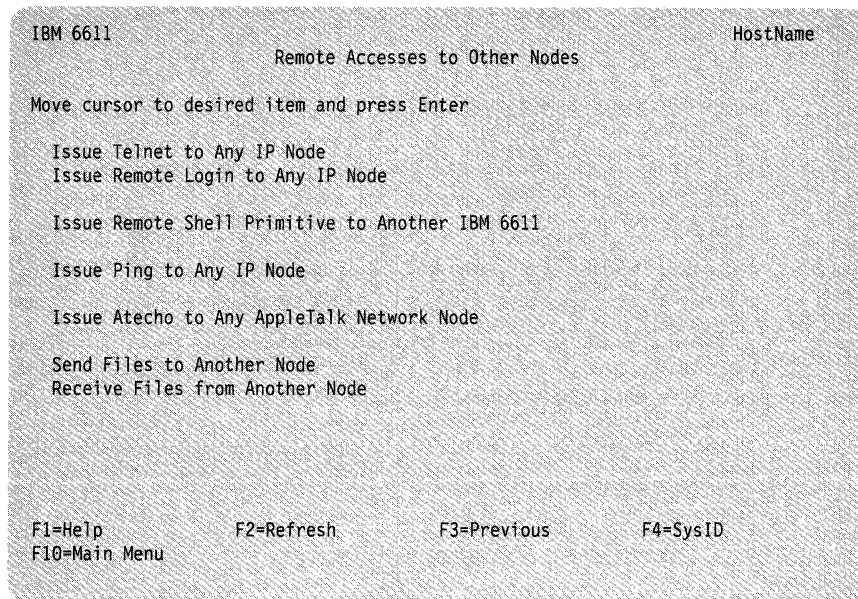


Figure 9-6. Remote Accesses to Other Nodes Menu

Using TELNET

TELNET is the most widely used method for one node on an IP network to reach another node. A user at a remote station can log in and interactively execute multiple commands at the destination station. Both IP stations must support TELNET for the session to be established. When a TELNET session is established to an IBM 6611, all the same tasks can be performed with the remote session as with the local attachment of the ASCII terminal to the EIA 232 serial ports.

Two TELNET session initiation procedures are outlined below:

- From a remote IP station to access an IBM 6611
- From one IBM 6611 to access any other IP station (including another IBM 6611).

Remote IP Station to IBM 6611: The IBM 6611 can be accessed from any station on the IP network using TELNET. The TELNET protocol requires you to know the host name or IP address, a userid, and a password configured for the IBM 6611. Userids and passwords must be configured using the Configuration Program, by a controlling user using the System Manager, or a fast-path environment primitive. See "Logging In to an IBM 6611" on page 9-23 for more information about IBM 6611 users.

The following steps show the details of a TELNET session's initiation from a remote station to an IBM 6611. You must have the *hostname* registered with the name server for the *hostname* to be recognized or the host name can be mapped to its IP address in the IBM 6611. (Refer to "Configuring Host Name to IP Address Mapping" on page 10-34 for more information.) What you are expected to input from the remote station is provided under **Type in**. What you should expect to find displayed on the screen is provided under **Output displayed**.

Type in:

```
telnet hostname
```

The IP address of the IBM 6611 can be used in the place of the host name.

Output displayed:

Trying...

Connected to hostname.domainname.

Escape character is '^T'.

IBM 6611 telnet (hostname)

```

=====  =====  =====  =====
=====  =====  =====  =====
==       ==       ==       ==
==       =====  =====  =====
==       =====  == =====  ==
==       ==       ==       =====
=====  =====  ==  ==  ==
=====  =====  ==  ==  ==
=====  =====  ==  =  =====

Multiprotocol Network Program
Welcome to the System Manager

```

(c)Copyrights by IBM and by others 1992

Login:

Type in:

userid

Output displayed:

userid's password:

Type in: (Enter the password. It will not be displayed.)

Output displayed:

```
The current terminal type is [sun].
Press the ENTER key to accept this value or
type NO to see a list of supported terminals.
```

Type in:

no

Output displayed:

SUPPORTED TERMINALS				

1. ibm3101	2. ibm3151	3. ibm3161	4. ibm3162	5. ibm3163
6. ibm3164	7. sun	8. vt100	9. vt320	10. vt330
11. vt340	12. hft			

Type the number corresponding to your choice:

Type in:

12

Output displayed: The main menu of the System Manager.

The last four steps can be eliminated if the remote station and the IBM 6611 negotiate the correct terminal type. At the completion of the login process, control is passed to the System Manager. If you exit the System Manager using **F10**

(**Esc + 0**) from the System Manager main menu, the remote connection is closed. In order to access the System Manager again you are required to reenter the **telnet** command.

See Chapter 7 for details about using the System Manager. If you want to execute IBM 6611 functions that require controlling user privileges, you must log in with a controlling userid. For more information about controlling user privileges, see "Logging In to an IBM 6611" on page 9-23.

IBM 6611 to Any IP Station: A TELNET session can also be initiated from the IBM 6611. This is accomplished with the System Manager or a fast-path environment command.

To initiate a TELNET session from an IBM 6611 to another IP station using the System Manager:

1. Select **Remote Accesses to Other Nodes** on the main menu.
2. Select **Issue Telnet to Any IP Node** on the next menu.

A dialog screen appears requesting the host name or IP address of the remote IP station being accessed. After entering the host name, you are prompted for a userid and password defined in the remote IP node. When the password you enter is correct, control is passed to the login environment of the remote station. See Chapter 7 for details about using the System Manager.

To initiate a TELNET session from the fast-path environment to another IP station, type:

```
telnet hostname
```

where *hostname* is the host name or IP address of the remote station. After issuing that command, you are prompted for a userid and password defined in the remote IP node. When the password is entered correctly, control is passed to the login environment of the remote station. See Chapter 8 for more information about using the fast-path environment.

Using Remote Login

There is an alternate method for one node on an IP network to reach another node on the IP network. It is called remote login, or RLOGIN. Using remote login, as with TELNET, a user at a station remote from another station can log in and interactively execute multiple commands at that station. Both stations must support RLOGIN in order to use this method. When a remote login session is established to an IBM 6611, all the same tasks can be performed from the remote session as with the local attachment of the ASCII terminal to the EIA 232 serial ports.

Two RLOGIN session initiation procedures are outlined below:

- From a remote IP station to access an IBM 6611
- From an IBM 6611 to access any other IP station (including another IBM 6611).

Remote IP Station to IBM 6611: The IBM 6611 can be accessed from any station on the IP network using the **rlogin** command, provided the station supports RLOGIN. The remote login requires you to know the host name or IP address and a userid and password configured for the IBM 6611. Userids and passwords must be configured using the Configuration Program, by a controlling user using the System Manager, or by a fast-path environment primitive. See "Logging In to an IBM 6611" on page 9-23 for more information about IBM 6611 users.

The following steps show the details of a remote login session initiation from a remote station to an IBM 6611. What you are expected to input from the remote station is provided under **Type in**. What you should expect to find displayed on the screen is provided under **Output displayed**.

Type in:

rlogin hostname (or IP address) -8 -l 6611_userid

The -8 instructs the **rlogin** command to use eight bit communication for data transfer. This is necessary when data is transferred over multiple nodes. The -l tells the **rlogin** command that the userid follows.

Output displayed:

userid's Password:

Type in: (Enter the password. It will not be displayed.)

Output displayed:

The current terminal type is [sun]. Press the ENTER key to accept this value or type NO to see a list of supported terminals.

Type in:

no

Output displayed:

SUPPORTED TERMINALS				

1. ibm3101	2. ibm3151	3. ibm3161	4. ibm3162	5. ibm3163
6. ibm3164	7. sun	8. vt100	9. vt320	10. vt330
11. vt340	12. hft			

Type the number corresponding to your choice:

Type in:

12

Output displayed: The main menu of the System Manager.

At the completion of the login process, control is passed to the System Manager. If you exit the System Manager using **F10 (Esc + 0)** from the System Manager main menu, the remote connection is closed. In order to access the System Manager again you are required to reenter the **rlogin** command.

IBM 6611 to Any IP Station: You can initiate also a remote login from the IBM 6611. This is accomplished with the System Manager or a fast-path environment command.

To issue the **rlogin** command from an IBM 6611 to another IP station on the same IP network using the System Manager:

1. Select **Remote Accesses to Other Nodes** on the main menu.
2. Select **Issue Remote Login to Any IP Node** on the next menu.

A dialog screen appears requesting:

- Host name (or IP address) of the remote IP node
- Userid.

After you have completed these required fields, you are prompted for the password of the userid given in the dialog. When you enter the password correctly, control is passed to the login environment of the remote station. If the remote IP station is

another IBM 6611, control is passed to the IBM 6611's System Manager. See Chapter 7 for information about using the System Manager.

To initiate a remote login session from the fast-path environment to another IP station, type:

rlogin hostname -8 -l userid

where:

- *hostname* is the host name or IP address of the remote station.
- The **-8** instructs the **rlogin** command to use eight bit communication for data transfer. This is necessary when data is transferred over multiple nodes.
- The **-l** tells the **rlogin** command that the *userid* follows. After issuing that command, you are prompted for the password of the *userid*. When you enter the password correctly, control is passed to the login environment of the remote station. See Chapter 8 for more information about using the fast-path environment.

Using RLOGIN for Extended Modem Connection

There are more IP stations supporting TELNET than RLOGIN. The IBM 6611 supports both methods. It is recommended that you use TELNET for most of your remote session needs. However, there is a particular situation in which an RLOGIN session is needed when a TELNET session cannot work. The scenario is explained using Figure 9-5 on page 9-5.

Scenario: A file needs to be transferred between IBM 6611-A and the station with the ASCII terminal that is modem attached to IBM 6611-B.

Procedure:

1. The user at the ASCII terminal initiates the call to IBM 6611-B and logs in to the IBM 6611, specifying *userid*, password, and terminal type when prompted.
2. From the System Manager main menu of IBM 6611-B that is automatically displayed at login completion:
 - a. Select **Remote Accesses to Other Nodes** on the main menu.
 - b. Select **Issue Remote Login to Any IP Node** on the next menu.
3. A dialog screen appears on which the user types in the host name and a *userid* at IBM 6611-A.
4. The user enters the password when prompted and control passes to the System Manager of IBM 6611-A.
5. There are several places in the System Manager that allow you to export specific files from IBM 6611-A. Each has an option to transfer the file using a modem. Select **Receive Files from Another Node** from this menu to import a file from the station that is modem-attached to IBM 6611-B.

If in Step 2, the user prefers to use TELNET instead of RLOGIN, the transfer cannot be made directly to the ASCII terminal. A technical difference between TELNET and RLOGIN allows data transfer across many nodes with RLOGIN and not with TELNET. This is the only situation in which RLOGIN is preferred over TELNET. See "Transferring Files" on page 10-43 for further details on file transfer.

Using Remote Execution

With TELNET and RLOGIN, you can have access to the full function of an IBM 6611. However, there are scenarios when this is not needed. If you only need to execute a single command at a remote IBM 6611, you can use remote execution (**rexec**). To use the **rexec** command, it must be supported by the IP station issuing the command.

The IBM 6611 supports the **rexec** command in conjunction with a specific set of command primitives. A large number of command primitives are supported. The primitives are listed in Chapter 8 along with the parameters needed to execute the command. Most functions that can be performed from the System Manager can also be performed using **rexec** and the command primitives without logging into the IBM 6611.

Each **rexec** command can execute one command primitive at the IBM 6611 to which the command is directed. The output from the command primitive is displayed at the station that issued the **rexec** command. The station that issues the command can be any station on the same IP network as the IBM 6611 to which the command is sent that supports remote execution.

Remote execution requires you to know the host name or IP address and a userid and password configured for the IBM 6611. Userids and passwords must be configured using the Configuration Program or by a controlling user using the System Manager or a fast-path environment command primitive. If you want to execute command primitives that require controlling user privileges, you are required to specify a controlling userid when prompted. For more information about the commands that require controlling user privileges, see “Logging In to an IBM 6611” on page 9-23. See Chapter 7 for information about using the System Manager.

The **rexec** command can be issued to the IBM 6611 from a remote IP station. The following steps show the details of a remote execution scenario from a remote station to an IBM 6611. Your input from the remote station is provided under **Type in**. The output that you should expect to see on the screen is provided under **Output displayed**.

Type in:

```
rexec hostname primitive parm1 parm2
```

The IP address of the IBM 6611 can be used in place of the host name.

Output displayed:

```
Name (hostname:local_userid):
```

Type in:

```
remote_userid
```

Output displayed:

```
Password (hostname:remote_userid):
```

Type in: (Enter the password. It will not be displayed.)

Output displayed: Command output follows, if any.

Many of the command primitives place the command output in the transfer directory of the IBM 6611 to which the command primitive is directed. If these primitives are issued from an RSH or REXEC environment, the **rsh** or **rexec** commands should be followed by an **ftp** to retrieve the output file.

Using Remote Shell

The remote shell (**rsh**) command can be used in a similar way to the **rexec** command. To use the **rsh** command, it must be supported by the IP station issuing the command. The IBM 6611 supports the **rsh** command in conjunction with a specific set of command primitives. A large number of command primitives are supported. The command primitives and the parameters are listed in Chapter 8. Most functions that can be performed from the System Manager can also be performed with **rsh** and the command primitives without logging in to the IBM 6611.

The **rsh** command executes command primitives one at a time at the IBM 6611 to which the command is directed. The output from the command primitives is displayed at the station at which the **rsh** command is issued. The station that issues the command can be any station on the same IP network as the IBM 6611 to which the command is sent.

As with remote execution, remote shell requires you to know the host name or IP address, and a userid and password configured for the IBM 6611. If you want to execute IBM 6611 functions that require controlling user privileges, you must specify a controlling userid. For more information about the commands that require controlling user privileges, see "Logging In to an IBM 6611" on page 9-23.

Two **rsh** command procedures are outlined below:

- From a remote IP station to access an IBM 6611
- From an IBM 6611 to access another IBM 6611.

Remote IP Station to IBM 6611: A typical situation for using a **rsh** command is within a script. A typical **rsh** command for the script is entered as follows:

rsh hostname -l userid passwd primitive parm1 parm2 ...

where:

- *hostname* is the host name of the IBM 6611 to which the command is sent. The *IP address* of the IBM 6611 can be used in place of the host name.
- *userid* is a userid defined at the IBM 6611 to which the command is sent.
- *passwd* is the password for the userid.
- *primitive parm1 parm2* is one of the supported command primitives and its parameters.

The output of the primitive is displayed at the station issuing the **rsh** command.

IBM 6611 to Another IBM 6611: You can also issue an **rsh** command from an IBM 6611 to another IBM 6611. This accomplished using the System Manager.

To issue remote shell from one IBM 6611 to another:

1. Select **Remote Accesses to Other Nodes** on the main menu.
2. Select **Issue Remote Shell Primitive to Another IBM 6611** on the next menu.

A dialog screen appears requesting:

- Host name or IP address of the IBM 6611
- Userid
- Password
- Command primitive
- Parameter for the command primitive.

Each of these fields can be edited using **F6 (Esc + 6)**. A pop-up edit screen is displayed with a long line on which to type the input. This is especially helpful when

typing in a primitive with a long name or several parameters. The parameters should be entered on the same line, separated by a space. See Chapter 7 for details about using the System Manager.

Many of the command primitives place the command output in the transfer directory of the IBM 6611 to which the command primitive is directed. If these primitives are issued from an RSH or REXEC environment, the **rsh** or **rexec** commands should be followed by an **ftp** to retrieve the output file.

Comparing REXEC and RSH

Remote execution and remote shell perform the same tasks using the command primitives. The main difference is in how you issue the commands. When the **rsh** command is sent to the IBM 6611, you are not prompted for the userid and password. The userid and password must be typed on the command line. This allows the **rsh** command and primitives to be combined in a user-written script containing more than one **rsh** command with or without the **ftp** command. This allows you to perform several functions while only issuing one script.

IBM suggests that you use REXEC when you need to execute an IBM 6611 command outside of a user-written script. This is because the password is not displayed as it is typed in after the prompt. With RSH, the password must be typed on the command line with the password in full view. If the screen output is saved, the password is also visible in the saved data.

Many of the command primitives place the command output in the transfer directory of the IBM 6611 to which the command primitive is directed. If these primitives are issued from an RSH or REXEC environment, the **rsh** or **rexec** commands should be followed by an **ftp** to retrieve the output file.

Using Ping

The **ping** command sends an Internet Control Message Protocol (ICMP) ECHO_REQUEST to obtain an ICMP ECHO_RESPONSE from another IP node. The **ping** command is useful to:

- Determine the status of the network and various remote stations
- Track and isolate hardware and software problems
- Test, measure, and manage networks.

If the station is operational and the station is on the IP network, it responds to the echo.

Each echo request contains an IP and ICMP header, followed by a time interval structure, and enough bytes to fill out the packet. It sends 1 datagram per second and prints 1 line of output for every response received. The **ping** command calculates round-trip times and packet loss statistics, and displays a brief summary upon completion. It completes after sending a specified number of echo requests.

A **ping** request can be sent from an IBM 6611 to any IP node on the network. This is accomplished using the System Manager or a fast-path environment command primitive.

To issue a **ping** request to any IP node from the System Manager:

1. Select **Remote Accesses to Other Nodes** on the main menu.
2. Select **Issue Ping to Any IP Node** on the next menu.

A dialog screen appears requesting:

- Host name (or IP address) of the IP node to ping.
- Number of **ping** requests to send.

See Chapter 7 for details on using the System Manager.

To issue a **ping** request from the fast-path environment to any IP node, type:

ping hostname number_bytes number_requests

where:

- *hostname* is the host name or IP address of the remote IP node
- *number_bytes* is the number of data bytes to send with each request
- *number_requests* is the number of **ping** requests to send.

See Chapter 8 for more information about using the fast-path environment.

Using Atecho for AppleTalk

The **atecho** command sends a request from an AppleTalk node. The **atecho** command is useful to:

- Determine the status of the network and various remote stations
- Track and isolate hardware and software problems
- Test, measure, and manage networks.

If the station is operational and the station is on the AppleTalk network, it responds to the echo.

Each echo request contains an AppleTalk DDP header, the **atecho** command, an identifier, and a sequence number, followed by a time interval structure, and enough bytes to fill out the packet. It sends 1 datagram per second and prints 1 line of output for every response received. The **atecho** command calculates round-trip times and packet loss statistics, and displays a brief summary upon completion. It completes after sending a specified number of echo requests.

An **atecho** request can be sent from an IBM 6611 to any AppleTalk node on the network. This is accomplished using the System Manager or a fast-path environment command primitive.

To issue an **atecho** request to any AppleTalk network from the System Manager:

1. Select **Remote Accesses to Other Nodes** on the main menu.
2. Select **Issue Atecho to Any AppleTalk Node** on the next menu.

A dialog screen appears requesting:

- Number of **atecho** requests to send
- AppleTalk network address
- AppleTalk node id.

See Chapter 7 for details on using the System Manager.

To issue an **atecho** request from the fast-path environment to any AppleTalk node, type:

atecho -c number_of_packets network_id node_id

Where:

- `-c` specifies the count field value option of the command.
- `number_of_packets` specifies the number of packets sent to a specific AppleTalk network address.
- `network_id` specifies the unique ID of the AppleTalk network address.
- `node_id` specifies the unique ID of the node that is on the AppleTalk network.

See Chapter 8 for more information about using the fast-path environment.

Using a Modem

Remote access to the IBM 6611 can also be reached through a modem that is connected to an EAI 232 serial port. The modem should be 2400 baud and compatible with the Attention (AT) Command Set. When the terminal is connected through the modem to the port, a login procedure is initiated. You are asked to supply the terminal type you are using immediately after login verification. After you have supplied the correct terminal type, the main menu of the System Manager is displayed.

When a connection is made using a modem, it is possible for you to access any IBM 6611 on the IP network using the network connection methods (**telnet**, **rlogin**, **rexec**, **rsh**, **ftp**, and **ping**). Therefore, you can have full remote modem access to any IBM 6611 on the network using only one modem connection. For most purposes, the single modem can be attached to an IP workstation instead of an IBM 6611 as long as the station supports **rlogin**.

When the modem connection is established, the call must be initiated from a station that is not an IBM 6611. The IBM 6611 does *not* support connection initiation. It can only receive the switched call.

There are three tasks you may need to perform to set up the modem connection physically:

1. Plug the modem into the S1 or the S2 EIA 232 serial port (labelled S1 and S1 on the Model 120 and Model 170, and labelled Serial 1 and Serial 2 on the Model 140).
2. Configure the serial port for a modem connection by changing the line speed (baud rate), if necessary.

The S1 or Serial 1 serial port is initially configured with a baud rate of 9600. If you need to change the baud rate, then you also need to reconfigure the port for use with a modem.

The S2 or Serial 2 serial port is initially configured for use with a modem with a baud rate of 2400. If you configure the port for use with Cylink through the Configuration Program, it cannot be used with a modem.

You can change the baud rate of the serial port with the System Manager or from the fast-path environment. To change the baud rate of the serial port using the System Manager, see "Configuring the EIA 232 S1 and S2 Serial Ports" on page 10-30. To change the baud rate of the serial port using the command primitives, see "Serial Port Command Primitives" on page 8-74.

3. Enable auto-answer mode for the modem.

The method for enabling auto-answer mode for the modem you purchased depends on the modem. Some modems may contain a physical switch for this function. Others require an AT command to be sent to the modem over the EIA 232 serial

port. Please read the documentation that accompanies the modem to see which method to use.

You can send an AT command to the modem to turn on auto-answer mode or to configure the modem for some other function using the System Manager. To send an AT command string using the System Manager:

1. Select **System Environment and Configuration** on the main menu.
2. Select **Send AT Command to Modem on Serial Port** on the next menu.
3. From the selector screen, select the EIA 232 serial port (**S1** or **S2**) to which the modem is attached.

A dialog screen appears requesting the command string. Press **F6 (Esc + 6)** to edit. A field edit screen appears with a line on which to type the command string. Press **Enter** after entering the command string to return to the dialog. Press **Enter** again to send the command to the modem. See Chapter 7 for details about using the System Manager. See Figure 10-8 on page 10-19 to see this functions on the System Environment and Configuration menu.

To establish a modem connection, you initiate the call from a remote station that supports call-out. If you want to transfer files, this station must also support the Xmodem protocol. Xmodem is available with many communication packages for personal computers and workstations. The communication package is used to access the IBM 6611's asynchronous serial line. Read the documentation sent with the communication package to understand the details of establishing the connection.

To establish a connection, you are required to know the telephone numbers and serial line parameters. See "Transferring Files between a RISC System/6000 and IBM 6611" on page 10-55 for information about the procedure for transferring files from a RISC System/6000 workstation using a modem connection.

When the connection to the IBM 6611 is established, you are prompted for a userid and password that have previously been configured for the IBM 6611 on the receiving end of the switched connection. See "Logging In to an IBM 6611" on page 9-23 for further discussion about the login procedure.

To access an IBM 6611, that is on the IP network but not equipped with a modem, it is necessary to establish an RLOGIN session between the IBM 6611 that needs to be accessed and the IP station on the network equipped with the modem. The remote login is initiated from the IBM 6611 or another IP node in the network equipped with the modem. If a node other than an IBM 6611 has the modem, it must support **rlogin** and **Xmodem** for transferring files. See "Using Remote Login" on page 9-10 for details of the remote login procedure.

Accessing the IBM 6611 through the EIA 232 Serial Ports

Two of the access configurations consist of a terminal attached either locally or remotely to one of the EIA 232 serial ports. Both EIA 232 serial ports are located at the rear of the IBM 6611 (labelled S1 and S2 on the Model 120 and Model 170, and labelled Serial 1 and Serial 2 on the Model 140). The attaching terminal must be a supported ASCII terminal or any terminal or workstation capable of emulating a supported ASCII terminal.

The IBM 6611 supports these ASCII terminal types, either specifically or by emulation:

- IBM terminals
 - IBM 3101
 - IBM 3151
 - IBM 3161
 - IBM 3162
 - IBM 3163
 - IBM 3164
- DEC terminals
 - VT100
 - VT320
 - VT330
 - VT340.

Note: If you use a personal computer that is configured to emulate one of the supported ASCII terminals, the display must support a 24 x 80 panel format (24 rows of 80 characters).

General Setup Attributes

Use Figure 9-7 to determine the settings for the general setup attributes for the IBM 3101 ASCII Terminal. Use Table 9-1 on page 9-20 to determine the settings for the general setup attributes for other ASCII terminals or terminal emulators.

Note: If you want to use an ASCII terminal or terminal emulator that does not emulate one of the IBM ASCII terminals, refer to the operator's manual for that device, compare its attributes with those in the table, and set them accordingly.

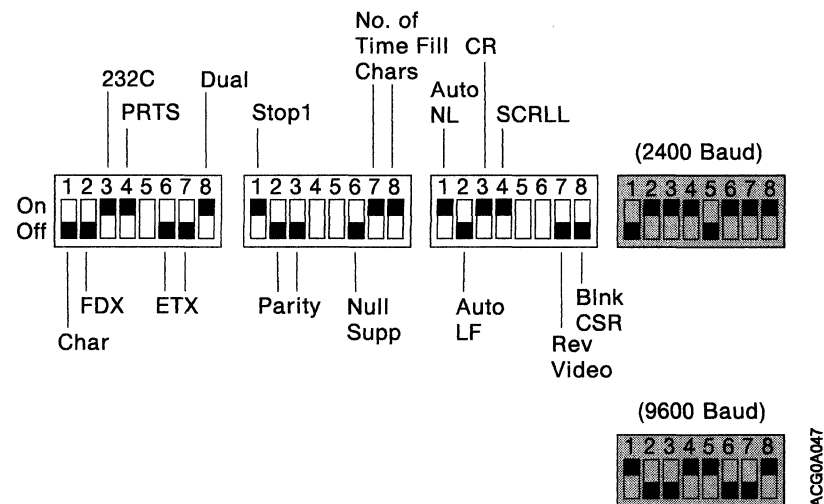


Figure 9-7. General Setup Attributes for the IBM 3101 ASCII Terminal

Table 9-1. General Setup Attributes for the ASCII Terminal or Emulator

General Setup Attributes	Settings	Explanations of the Settings
Row and Column	24 x 80	The screen format is 24 rows of 80 characters.
Scroll	Jump	When the last character on the last line of the screen is received or entered, all of the lines on the screen move up one line.
Auto LF	Off	For the Off setting, pressing Return moves the cursor to the first character position of the current line. The carriage return (CR) and the line feed (LF) characters are generated by the setting for the New Line attribute.
CRT saver	Off	The 10 setting causes the display screen to go blank if there is no activity for 10 minutes. When the IBM 6611 sends data or a key is pressed, the information on the screen is displayed again.
Line wrap	On	The cursor moves to the first character position of the next line on the screen after it reaches the last character position of the current line on the screen.
Forcing insert	Off	If there is no space to insert a character or a null line, an insert operation cannot be performed.
Tab	Field	The column tab stops are ignored, and tab operation depends on the field attribute character positions.
Trace	All	Both inbound data (data to the IBM 6611) and outbound data (data from the IBM 6611) to and from the main port can be transferred to the terminal's auxiliary port without disturbing communications with the IBM 6611 when Trace is pressed.

Communication Setup Attributes

Table 9-2 on page 9-21 list most of the terminal and EIA 232 serial port characteristics. The IBM 6611 setting is given along with an explanation of the parameter. Most terminal emulators allow you to change these settings. The only attribute that is configurable from the IBM 6611 is the line speed (baud rate). These can be set from the Configuration Program, or the System Manager. See "Configuring the EIA 232 S1 and S2 Serial Ports" on page 10-30 for instructions, recommendations, and requirements about setting the baud rate for the serial ports.

The settings for the attributes in Table 9-2 are based on the assumption that the ASCII terminal or terminal emulator is directly connected to the S1 or S2 serial port of the IBM 6611. If the ASCII terminal communicates with the IBM 6611 via a modem that is connected to the serial port, a different setting for some attributes may be required. An arrowhead (➤) indicates those attributes that may require different settings. The appropriate setting would depend on the type of modem and the communications line.

Table 9-2 (Page 1 of 2). Communication Setup Attributes for the ASCII Terminal or Emulator

Communication Setup Attributes	Settings	Explanations of the Settings
Operating mode	Echo	Data entered from the keyboard on the terminal is sent to the system unit for translation and then sent back to the display screen. Echo mode is also called <i>conversation mode</i> .
Line speed▶	1200,2400,9600, 19200,38400	Uses 9600-bps, 19200-bps, or 38400-bps line speeds to communicate with the IBM 6611 for a direct-attached terminal. Uses 1200-bps or 2400-bps line speeds to communicate with the IBM 6611 for a modem-attached terminal. See "Configuring the EIA 232 S1 and S2 Serial Ports" on page 10-30 for information about how to configure the EIA serial ports.
Word length (bits)	8	The data word length is 8 bits.
Parity	No	Does not add a parity bit, and is used together with the word length attribute to form the 8-bit data word (byte).
Stop bit	1	Places a bit after a data word.
Turnaround character	CR	The carriage return (CR) character is used as the line turnaround character.
Interface	RS232C	Uses the EIA 232-C electrical interface protocol.
Line control▶	IPRTS	Uses the permanent request to send (IPRTS) signal to communicate with the IBM 6611.
Break signal▶	500	The terminal sends a 500-ms break signal to the IBM 6611 after Break is pressed.
Send null suppress (if supported)	On	The terminal does not send trailing null characters to the IBM 6611.
Send null (if supported)	On	The terminal sends trailing null characters to the IBM 6611.
Response delay▶	100	The terminal waits 100-ms for the IBM 6611 to respond.
Enter	Return	The Enter key functions as the Return key.
Return	New line	The cursor moves to the next unprotected field when Return is pressed.
New Line	CR	The Return key generates the carriage return (CR) and the line feed (LF) characters. The line turnaround occurs after the CR and LF characters are generated.
Send	Page	The contents of the current page are sent to the IBM 6611 when the Send key is pressed.
Insert character	Space	A blank character is inserted when Insert is pressed.

Table 9-2 (Page 2 of 2). Communication Setup Attributes for the ASCII Terminal or Emulator

Communication Setup Attributes	Settings	Explanations of the Settings
xon-xoff handshaking	yes	This parameter indicates whether inbound data is to be searched for start and stop characters as a method of allowing devices to control the output they are receiving, and whether stop and start characters are to be placed in the outbound data stream to attempt to control the output the system is receiving from terminal devices. The possible choices are yes or no.
interrupt character	Ctrl + C	This parameter defines the interrupt special character that is recognized on input. The interrupt character generates an interrupt signal that is sent to all running programs for which the port is the controlling workstation.
quit character	Ctrl + \	This parameter defines the quit special character that is recognized on input. The quit character generates a quit signal that is sent to all running programs for which the port is the controlling workstation.
erase character	Ctrl + h	This parameter defines the special character that is used to erase characters from the input stream. The erase character does not erase past the end of the line as delimited by an NL, EOL, or EOF character.
kill character	Ctrl + u	This parameter indicates the kill special character that is recognized on input. The kill character deletes the entire line from the input stream, as delimited by an NL, EOL, or EOF character.
EOF character	Ctrl + d	This parameter indicates the special character that is recognized on input and is used to indicate the end of an input stream. When the EOF special character is received, all the characters waiting to be read are immediately passed to the program.
EOL character	Ctrl + @	This parameter indicates the special character that is recognized on input and is used to indicate the end of line in an input stream.
Start character	Ctrl + q	This parameter indicates the special start character that is recognized on input and output and is used to resume output that has been suspended by a stop character.
Stop character	Ctrl + s	This parameter indicates the special character that is recognized on input and output and is used to stop output that is scrolling past the terminal. Suspended output can be resumed by using the start character.
Enable login	Yes	This parameter allows a user to log in over the serial port.

Transferring Files with Serial Port Access

If you have accessed your IBM 6611 using the EIA 232 serial ports, you are either directly connected or connected through a modem. With direct connection you can transfer files to or from a diskette. With modem connection you can transfer files to or from the remote node using the Xmodem protocol. The details of transferring files using these methods will not be covered here. For further information consult the following references:

1. "Performing Diskette Operations" on page 10-22
 - "Formatting a DOS or UNIX Diskette" on page 10-23
 - "Listing Files on a DOS or UNIX Diskette" on page 10-24
 - "Importing Files From a DOS or UNIX Diskette" on page 10-24
 - "Exporting Files to a DOS or UNIX Diskette" on page 10-25
 - "Diskette Operations on a Model 170 With 7 Peer-Capable Adapters" on page 10-25
2. "Transferring Files" on page 10-43
 - "Exporting Specific Data" on page 10-50
 - "Importing Specific Data" on page 10-51
 - "Exporting Files to a Remote Node" on page 10-52
 - "Importing Files from a Remote Node" on page 10-52
 - "Using the Xmodem Protocol" on page 10-55

Logging In to an IBM 6611

The login procedure for the IBM 6611 is the same, if you are local or remote and using a network connection or a modem connection. You are prompted for a userid, password, and terminal type. The login scenario for remote access via TELNET is found in "Using TELNET" on page 9-8. The login scenario for remote access via RLOGIN is found in "Logging In to an IBM 6611."

The following steps show the details of the login procedure from a terminal connected to the S1 or S2 serial port, either directly or through a modem. Your input from the ASCII terminal is provided under **Type In**. The output that you should expect to see displayed on the screen is provided under **Output displayed**.

Output displayed:

Multiprotocol Network Program

Welcome to the System Manager

(c)Copyrights by IBM and by others 1992

Login:

Type in:

userid

Output displayed:

userid's password:

Type in: (Enter the password. It will not be displayed.)

Output displayed:

```
The current terminal type is [vt100].
Press the ENTER key to accept this value or
type NO to see a list of supported terminals.
```

Type in:

no

Output displayed:

SUPPORTED TERMINALS				
-----		-----		
1. ibm3101	2. ibm3151	3. ibm3161	4. ibm3162	5. ibm3163
6. ibm3164	7. sun	8. vt100	9. vt320	10. vt330
11. vt340	12. hft			

Type the number corresponding to your choice:

Type in:

6

Output displayed: The main menu of the System Manager.

When logging in through the EIA 232 serial ports the terminal type chosen on the previous login is presented as the default type. It is assumed that the terminal type used for this connection is normally the same from login to login.

At the completion of the login process, control is passed to the System Manager. If you exit the System Manager using **F10 (Esc + 0)** from the System Manager main menu, you will return to the login prompt. See Chapter 7 for details on using the System Manager.

Userids and Passwords

There are two classes of IBM 6611 users:

- Viewing class
- Controlling class.

Users with viewing privileges cannot perform all the operations of the IBM 6611. Full privileges are given to the controlling class.

Only 10 system users can be logged into the IBM 6611 at the same time. However, it is recommended that you allow a maximum of five users to minimize the impact to system performance. Userids and passwords are defined using either the Configuration Program, the System Manager, or the command primitives. Both the userid and the password must be defined together, if initially defined from the Configuration Program.

Two default userids are preconfigured with the IBM 6611. One is a controlling userid and the other is a viewing userid. The controlling userid and password is `ibm6611c`. The viewing userid and password is `ibm6611v`. IBM recommends that you delete these userids or change the passwords immediately after receiving the IBM 6611. The default userids are to be used during initial configuration of the IBM 6611, if performed using the System Manager. See "Initial Configuration without Using a Diskette" on page 14-11 for details about using the System Manager for initial configuration.

From the System Manager you can list all the users, add a user, delete a user and change user passwords, if you have controlling class privileges. See "Configuring Userids and Passwords" on page 10-31 for details of setting userids and passwords.

Controlling User Tasks

Many of the System Manager functions require controlling user privileges. If you attempt to execute a System Manager function from a viewing userid that requires controlling user privileges, you will receive a message similar to the one shown here:

Only a controlling user can perform this function.

The following names list all the functions that only a controlling user can perform. Each of the menu items is listed under the main menu item under which it appears.

- Performance and Statistics
 - View System Activity Report
 - View Process Table Information
 - View Virtual Memory Statistics
 - View Input/Output Statistics
 - View Protocol and Interface Packet Traffic Information
- Problem Determination Facilities
 - Clean the Error Log
 - Start System Dump
 - View Previous System Dump Information
 - Copy System Dump to Diskette or Transfer Directory
 - View a Formatted System Dump
 - Extract Error Log Records From System Dump
 - Extract Trace Log Records From System Dump
 - Start APPN User Process Memory Dump
 - Start User Process Memory Dump

- Start IP Routing Protocols Dump
- Start System Trace
- Stop System Trace
- Start IP Routing Protocols Trace
- Stop IP Routing Protocols Trace
- Start APPN Trace
- Stop APPN Trace
- Start AppleTalk Protocol Trace
- Stop AppleTalk Protocol Trace
- Start and Stop SNMP Trace
- Read Adapter Memory
- View Adapter Registers
- Start Adapter Line Trace
- Dump Adapter Memory
- Concurrent Hardware Diagnostics
- Resource Control and Management
 - Stop the System With or Without Re-IPL
 - Read Three-Digit Display on Operator Panel
 - Add System ARP Entry
 - Delete System ARP Entry
 - Add Adapter ARP Entry
 - Delete Adapter ARP Entry With Hardware Address
 - Delete Adapter ARP Entry With Host Name
 - Clear Adapter ARP Table
- System Environment and Configuration
 - Work with Files in Transfer Directory - rename
 - Work with Files in Transfer Directory - delete
 - Configure EIA/232 Serial Ports
 - Send AT Command to Modem on Serial Port
 - Show and Change Date and Time
 - Change Date, Time, and Time Zone
 - Add a User
 - Delete a User
 - Change User Password
 - Change Your Password
 - Set Host Name Information
 - Add a Host Name to the Mapping
 - Delete a Host Name from the Mapping
 - Start Using Name Service
 - Stop Using Name Service
 - Add a Name Server
 - Delete a Name Server
 - Start Using Time Service
 - Stop Using Time Service
 - Add a Time Server
 - Delete a Time Server
 - Apply Changes to Configuration Database
 - Commit Changes to Configuration Database
 - Reject Uncommitted Changes to Configuration Database
- Software Installation and Maintenance
 - Import Software to Transfer Directory
 - List All Software in the Transfer Directory

- List All Problems Fixed by Software Updates in Transfer Directory
- Apply Software Components
- Apply Software Updates
- List All Applied but Not Committed Software
- Commit Applied Updates (Delete Previous Version)
- Reject Applied Updates (Use Previous Version)
- Remove Saved Software Component
- Reinstate Saved Software Component
- Clean Up After a Failed Installation
- Verify a Software Component
- Hardware Vital Product Data
 - Update Hardware Vital Product Data After Configuration Changes
- Configuration Files and Reports
 - Import Binary Configuration File
- Adapter and Protocol Configuration
 - Show Configuration Values for Single Objects
 - Set Configuration Values for Single Objects
 - Add Configuration Element to a List Object
 - Delete Configuration Element from a List Object
 - List Configuration Elements in a List Object
 - Apply Changes to Configuration Database
 - Commit Changes to Configuration Database
 - Reject Uncommitted Changes to Configuration Database

Chapter 10. Operating the IBM 6611

About This Chapter	10-3
Performing Resource Control and Management Tasks	10-3
Starting the IBM 6611	10-4
Stopping the IBM 6611	10-4
Reading the Three-Digit Display	10-6
Viewing the System Route Table	10-7
Viewing the Adapter Route Tables	10-9
Viewing the Network Management Subsystem Information	10-11
Managing ARP Tables	10-13
Viewing System ARP Entries	10-14
Adding a System ARP Entry	10-14
Deleting a System ARP Entry	10-15
Viewing Adapter ARP Entries	10-15
Adding an Adapter ARP Entry	10-15
Deleting an Adapter ARP Entry with Hardware Address	10-16
Deleting an Adapter ARP Entry with Host Name	10-17
Clearing the Adapter ARP Table	10-17
Viewing Adapter AARP Entries	10-17
Exporting the Route Table Information	10-18
Performing System Environment and Configuration Tasks	10-18
Working with Files in the Transfer Directory	10-19
Viewing a File in the Static Directory	10-21
Sending an AT Command to a Modem Attached to an EIA 232 Serial Port	10-22
Performing Diskette Operations	10-22
Formatting a DOS or UNIX Diskette	10-23
Listing Files on a DOS or UNIX Diskette	10-24
Importing Files From a DOS or UNIX Diskette	10-24
Exporting Files to a DOS or UNIX Diskette	10-25
Diskette Operations on a Model 170 With 7 Peer-Capable Adapters	10-25
Attaching a Workstation Capable of Diskette Operations to a EIA 232 Serial Port	10-25
Reconfiguring the Model 170 to Enable the Diskette Drive	10-26
Showing and Changing the Date and Time	10-26
Changing the Date, Time, and Time Zone	10-27
Performing System Configuration Changes	10-28
Configuring the EIA 232 S1 and S2 Serial Ports	10-30
Configuring Userids and Passwords	10-31
List All Users	10-33
Add a User	10-33
Delete a User	10-33
Change User Password	10-34
Change Your Password	10-34
Configuring Host Name to IP Address Mapping	10-34
Setting Host Name Information	10-35
Listing All Static Host Name Mappings	10-36
Adding a Host Name to the Mapping	10-36
Deleting a Host Name from the Mapping	10-36
Configuring Remote Host Name Service	10-37
Listing All Name Servers	10-37
Start Using the Name Service	10-38
Stop Using the Name Service	10-38
Adding a Name Server	10-38

Deleting a Name Server	10-39
Configuring Remote Time Service	10-39
Listing All Time Servers	10-40
Start Using Time Service	10-40
Stop Using Time Service	10-40
Adding a Time Server	10-41
Deleting a Time Server	10-41
Apply Changes to Configuration Database	10-41
Commit Changes to Configuration Database	10-42
Reject Uncommitted Changes to Configuration Database	10-42
Transferring Files	10-43
File Names for Output in Transfer Directory	10-43
Exporting Specific Data	10-50
Importing Specific Data	10-51
Exporting Files to a Remote Node	10-52
Importing Files from a Remote Node	10-52
Using the File Transfer Protocol	10-52
Using the Xmodem Protocol	10-55
Transferring Files between a RISC System/6000 and IBM 6611	10-55
Transferring Files to Diskette	10-57
Selling the IBM 6611 to a Third Party	10-57

About This Chapter

This chapter describes how to use the System Manager to execute most of the tasks needed for operating the IBM 6611. You can use the Resource Control and Management and System Environment and Configuration menus to perform these tasks. The explanation for these tasks are in “Performing Resource Control and Management Tasks” and “Performing System Environment and Configuration Tasks” on page 10-18, respectively. This chapter also contains information about “Transferring Files” on page 10-43.

Performing Resource Control and Management Tasks

Figure 10-1 displays the Resource Control and Management menu. You can access the Resource Control and Management menu from the main menu of the System Manager.

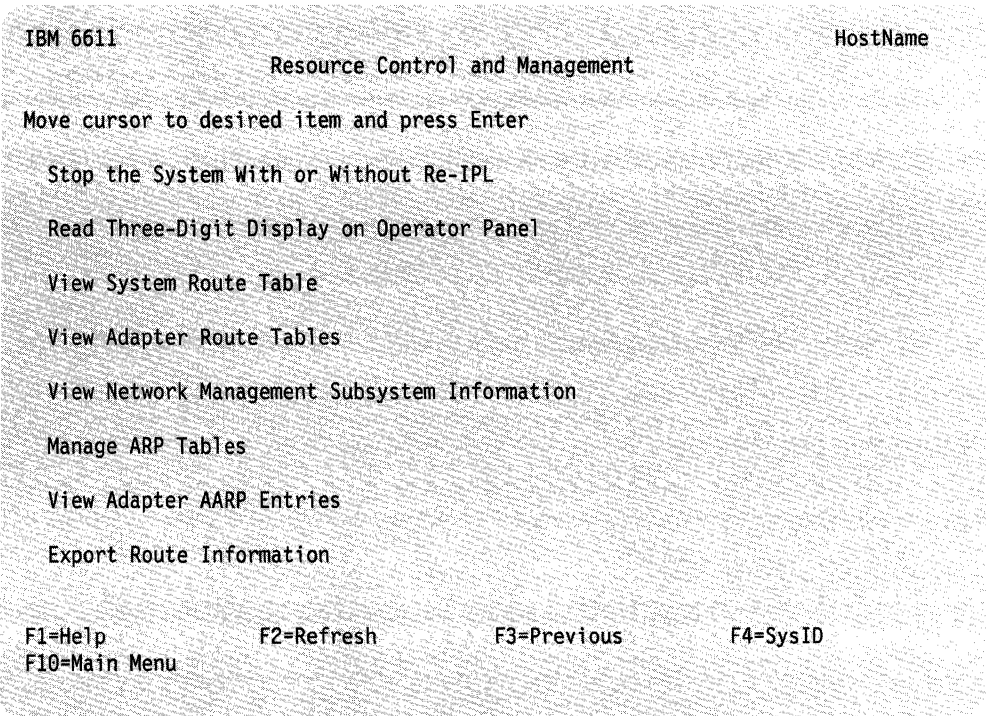


Figure 10-1. Resource Control and Management Menu

The Resource Control and Management menu allows you to control and manage many of the major hardware and software components of the IBM 6611. The following sections explain how to access these tasks using the System Manager.

See the following pages for more information about these procedures.

Starting the IBM 6611	10-4
Stopping the IBM 6611	10-4
Reading the Three-Digit Display	10-6
Viewing the System Route Table	10-7
Viewing the Adapter Route Tables	10-9
Viewing the Network Management Subsystem Information	10-11
Managing ARP Tables	10-13

Viewing Adapter AARP Entries	10-17
Exporting the Route Table Information	10-18

Starting the IBM 6611

You can start the IBM 6611 two ways:

- Using the power switch
- Using the Reset push button.

You can stop or restart the IBM 6611 using the System Manager or command primitives. See "Stopping the IBM 6611" for details.

To start the IBM 6611:

1. Set the key mode switch to **Normal**.
2. Start the IBM 6611, by setting the power switch to **ON (I)**.

When you set the power switch to **ON (I)**, the power-on light comes on and the IBM 6611 starts a power-on self-test (POST). During the POST, numbers are displayed on the 3-digit display.

3. If the power-on light does not come on, check the power cord that is located at the back of the IBM 6611 to ensure that it is plugged into a grounded electrical wall outlet. If this does not solve the problem, contact IBM service personnel.

To restart an IBM 6611, when the IBM 6611 is powered on:

1. Set the key mode switch to **Normal**.
2. Press the **Reset** push button causing the IBM 6611 to reset and restart the system.

Note: If the IBM 6611 has a flashing **888** on the 3-digit display, pressing the Reset button displays additional codes or diagnostic messages. When this happens, turn the power switch to OFF (O) for one minute, then turn it to ON (I) again to start the IBM 6611.

Stopping the IBM 6611

There are times when it is necessary to stop the operation of the IBM 6611. Do not stop operations by turning the power switch to Off (O). There is a command to shut down the IBM 6611 that performs all necessary cleanup operations. The **shutdown** command stops all operations in the base operating system, including all routes needing to access the main system and all user sessions. This command does not stop the operation of the peer-capable adapters, just their communication with the main operating system. After the system has been stopped with the **shutdown** command, you can power off the IBM 6611. Turning off the power is the only method of stopping the peer-capable adapters.

Prior to beginning the shutdown, you will receive a message including the number of minutes before the system is shut down. There is a series of messages displayed during the shutdown process. These messages vary slightly depending on whether you are connected over an EIA 232 serial port or a remote network connection, such as, TELNET and whether or not you asked to restart the system immediately after shutdown.

You receive the following messages over a direct connection without the restart option specified.

SHUTDOWN PROGRAM
Sun Dec 22 18:07:50 1991

Broadcast message from ibm6611c on tty ...

PLEASE LOG OFF NOW !!!

System maintenance in progress.
All processes will be terminated in 3 minutes.

Broadcast message from ibm6611c on tty ...

THE SYSTEM IS BEING BROUGHT DOWN NOW

Wait for '...Halt complete ...' before stopping.
Process accounting has stopped.
Error reporting has stopped.
Stopping NFS/NIS Daemons
The Subsystem or Group, nfsd, is currently inoperative.
The Subsystem or Group, biod, is currently inoperative.
The Subsystem or Group, rpc.lockd, currently inoperative.
The Subsystem or Group, rpc.statd, currently inoperative.
The Subsystem or Group, rpc.mountd, currently inoperative.
The Subsystem or Group, yppasswdd, currently inoperative.
The Subsystem or Group, ypupdated, currently inoperative.
All processes currently running will now be terminated.
Halt complete ...

The last two lines are not displayed if the system shutdown command is issued from a remote user over a TELNET session.

Do not attempt to restart the system or turn off the IBM 6611 before the shutdown completion message is displayed. Otherwise, file system damage can result.

Only a controlling user can shut down the IBM 6611.

To stop the IBM 6611 with the option to restart from the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Resource Control and Management** from the main menu.
3. Select **Stop the System With or Without Re-IPL** from the next menu.
4. From the dialog screen, select **yes** or **no** to indicate whether or not you want to restart the system after the shutdown. Enter the elapsed time, in minutes, when the system begins to shut down.

5. You receive the following two messages warning you of the results of shutting down your IBM 6611:

ARE YOU SURE?

Executing this command will shut down your IBM 6611, stopping all the protocols and processes including the current System Manager session.
Press Enter to shutdown the IBM 6611.
Press Previous to cancel and return to the System Manager.

F1=Help F2=Refresh F3=Previous
F10=Main Menu

INFORMATION MESSAGE

NOTE: This command needs to be run outside of the System Manager.
Therefore the System Manager will exit immediately before running this command.

Press Enter to proceed with the command.

Press Previous to cancel and return to the System Manager.

F1=Help F2=Refresh F3=Previous
F10=Main Menu

To continue with the system shutdown, press **Enter**.

You can invoke this task using command primitives. See "Shutdown: System Command Primitives" on page 8-76 for information about the command primitives.

Reading the Three-Digit Display

To retrieve error or status codes which appear on the 3-digit display using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Resource Control and Management** on the main menu.
3. Select **Read Three-Digit Display on Operator Panel** from the next menu.

You receive a command status screen with the error or status code displayed along with its meaning and user response. See "3-Digit Display Command Primitive" on page 8-100 for a description of the command primitive for viewing the error and status codes. For more information about the error and status codes, see Appendix B.

Figure 10-2 shows an example of the output displayed from reading the 3-digit display using the System Manager.

Code: 10c
Message: The system monitor process cannot access the adapter installed in slot 1 due to a problem with:

- System code that communicates with the adapter.
- Adapter microcode.
- Adapter hardware.

User Response/Action: For suspected software problem (CE):

- Check error log to determine software problem.

For suspected hardware problem (CE):

- Execute adapter diagnostics.
- Check the adapter for proper installation.
- Check the adapter for defects.

Figure 10-2. Sample Output from Reading the 3-Digit Display

Viewing the System Route Table

The system route table contains the routes for most of the configured protocols in the IBM 6611. The route tree is shown for each protocol family. The supported protocols are:

IP	Protocol Family 2
IPX	Protocol Family 26
XNS	Protocol Family 6
LAN Bridging Protocol	Protocol Family 27
Spanning Tree	Protocol Family 27
DECnet	Protocol Family 12
AppleTalk	Protocol Family 16

The display format indicates the available routes and their states. Each route consists of a destination host or network and a gateway to use when forwarding packets. Direct routes are created for each interface attached to the local host. The routing table contains the following six fields:

destination The IP address or host name at the end of the route.

gateway The gateway field for these entries shows the address of the outgoing interface.

flags The flags field of the routing table shows the state of the route:

U Up

H The route is to a host rather than to a network.

G The route is to a gateway.

D The route was created dynamically by a redirect.

- M** The route has been modified by a redirect.
- L** The link-level address is present in the route entry.
- refcnt** Gives the current number of active uses for the route. Connection-oriented protocols hold on to a single route for the duration of a connection, while connectionless protocols obtain a route while sending to the same destination.
- use** Provides a count of the number of packets sent using that route.
- interface** Indicates the network interfaces utilized for the route. See Table 10-1 for an explanation of the interface name.

Table 10-1. Adapter Interface Name Table

Adapter or Interface	Interface Name
Token-Ring Network 16/4 Adapter	tk#
Ethernet Adapter	te#
EIA 422/449 Serial Adapter	to?
V.35/V.36 Serial Adapter	to?
X.25 Adapter	xt#
Loopback	lo\$

The number sign (#) is a number from 0 to 6. The question mark (?) is a number from 0 to 13. The dollar sign (\$) is either 0 or 1. The number corresponds to the order of that particular adapter type or adapter port as it is located in the IBM 6611. For example, *te0* corresponds to the first Ethernet adapter and *to1* corresponds to the second Serial adapter port. Loopback is an internal interface that the IBM 6611 uses to test its own network availability.

You can invoke this task using command primitives. See “Route Table Command Primitives” on page 8-73 for information about the command primitives.

To view the system route table using the System Manager:

1. Select **Resource Control and Management** from the main menu.
2. Select **View System Route Table** from the next menu.
3. Select the destination of the route table (**screen** or **transfer_directory**) from the selector screen.
4. The system route table is displayed.

Figure 10-3 on page 10-9 shows an example of output obtained by viewing the system route table from the System Manager.

```

Routing tables
Destination      Gateway          Flags          Refcnt Use    Interface
Netmasks:
(root node)
(0) 0 ffff ff00 0
(root node)

Route Tree for Protocol Family 2:
(root node)
6611host         8.8.8.2         UH             1          1   to0
9.66.23          9.66.23.8       U              1         196  tk0
9.66.31          9.66.31.8       U              1         887  te0
loopback         loopback        UH            12        12255 lo0
(root node)

Route Tree for Protocol Family 6:
(root node)
(root node)

```

Figure 10-3. View System Route Table Example

Viewing the Adapter Route Tables

Each of the peer-capable adapters have their own route tables. The adapter route table display format indicates the available routes and status. Each route consists of a destination host or network and a gateway to use to forward packets. The routing table contains the following four fields:

- destination** The IP address or host name at the end of the route.
- gateway** The gateway field for these entries shows the address of the outgoing interface.
- flags** The flags field of the routing table shows the state of the route:
- U** Up
 - H** The route is to a host rather than to a network.
 - G** The route is to a gateway.
 - D** The route was created dynamically by a redirect.
 - M** The route has been modified by a redirect.
 - L** The link-level address is present in the route entry.
- interface** Indicates the network interfaces used for the route.

This command displays information about the configuration of the network management subsystem. This is useful as problem solving information. The displayed information includes the following:

- State of the SNMP process trace flags
- Maximum SNMP packet size
- SNMP query timeout
- SNMP subagent timeout
- All configured communities
- All configured views
- All configured subagents
- All configured SNMP trap destinations.

See Table 10-1 on page 10-8 for an explanation of the interface names.

You can invoke this task using command primitives. See "Route Table Command Primitives" on page 8-73 for information about the command primitives.

To view the adapter route tables using the System Manager:

1. Select **Resource Control and Management** from the main menu.
2. Select **View Adapter Route Tables** from the next menu.
3. Select the peer-capable adapter interface name for the route table you want to view from the selector screen. See Table 10-1 on page 10-8 for an explanation about the interface name used to identify the adapters. This command is only valid for the peer-capable adapters:
 - Token-Ring Network 16/4 Adapter
 - Ethernet Adapter
 - EIA 422/449 Serial Adapter
 - V.35/V.36 Serial Adapter.
4. Select the protocol whose route table you want to view from the next selector screen. The protocols supported are:
 - Internet
 - XNS
 - IPX
 - DECnet
 - AppleTalk.
5. Select the destination of the route table (**screen** or **transfer_directory**) from the next selector screen. You receive the adapter route table.

Figure 10-4 shows an example of the output obtained by viewing an adapter route table from the Internet Protocol.

Destination	Gateway	Flags	Interface
6611host	8.8.8.2	UH	to0
8.8.8.2	loopback	UH	lo0
8.8.8.255	loopback	UH	lo0
9.66.23	9.66.23.8	U	tk0
9.66.31	9.66.31.8	U	te0
9.66.23.8	loopback	UH	lo0
9.66.31.8	loopback	UH	lo0
255.255.255.255	loopback	UH	lo0
8.255.255.255	loopback	UH	lo0
9.66.23.255	loopback	UH	lo0
9.66.31.255	loopback	UH	lo0
9.255.255.255	loopback	UH	lo0

Figure 10-4. Adapter Route Table Example

Viewing the Network Management Subsystem Information

This command displays information about the configuration of the network management subsystem. This is useful problem solving information. The displayed information includes the following:

- State of the SNMP process trace flags
- Maximum SNMP packet size
- SNMP query timeout
- SNMP subagent timeout
- All configured communities
- All configured views
- All configured subagents
- All configured SNMP trap destinations.

To obtain this information using the System Manager:

1. Select **Resource Control and Management** from the main menu.
2. Select **View Network Management Subsystem Information** on the next menu.
3. Select output destination (**screen** or **transfer_directory**) from the screen.

Figure 10-5 on page 10-12 shows an example of the output you receive when you request the network management subsystem information.

```
Logfile:      /tmp/hold/transfer/pd_snmpd.log
Tracing:      ENABLED          ACTIVE
Debug level:  0
Max Packet Size:9216
Query Timeout: 60
SMUX Timeout: 15
COMMUNITY:    public
  ADDRESS:    127.0.0.1
  NETMASK:    255.255.255.255
  PERMISSION: readOnly
  VIEW:       1.3.6.1.3.11.2.2
COMMUNITY:    public
  ADDRESS:    0.0.0.0
  NETMASK:    255.255.255.255
  PERMISSION: readOnly
  VIEW:       1.3.6.1.3.11.2.2
VIEW NAME:    1.3.6.1.3.11.2.1
  SUBTREE(S): iso
VIEW NAME:    1.3.6.1.3.11.2.2
  SUBTREE(S): iso
  SUBTREE(S): mgmt
  SUBTREE(S): mgmt
VIEW NAME:    1.3.6.1.3.11.2.5.1
  SUBTREE(S): iso
TRAP DESTINATION
public          9.66.23.4
SMUX CLIENT:   1.3.6.1.4.1.2.3.1.2.1.2
  PASSWORD:    gated_password
  ADDRESS:     127.0.0.1
  NETMASK:     255.255.255.255
SMUX CLIENT:   1.3.6.1.4.1.2.6.2.1.1
  PASSWORD:    Route66
  ADDRESS:     127.0.0.1
  NETMASK:     255.255.255.255
SMUX CLIENT:   1.3.6.1.4.1.2.6.2.1.2
  PASSWORD:    Route66
  ADDRESS:     127.0.0.1
  NETMASK:     255.255.255.255
```

Figure 10-5. Example of View Network Management Subsystem Information Output

Managing ARP Tables

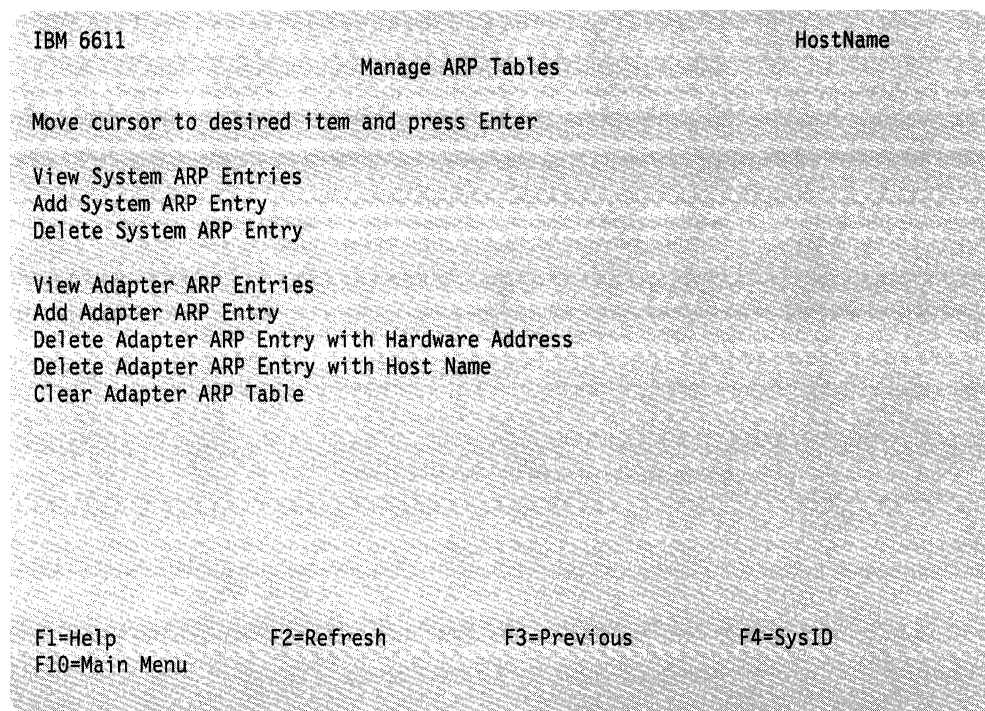


Figure 10-6. Manage ARP Tables Menu Screen

The Address Resolution Protocol (ARP) translates unique IP addresses into unique hardware addresses. Tables in the main operating system and on each of the Token-Ring and Ethernet peer-capable adapters store the mapping of the hardware address to its host name or IP address. You can view the tables and add or delete entries from the tables.

To manage address resolution protocol (ARP) tables using the System Manager:

1. Select **Resource Control and Management** from the main menu.
2. On the next menu, select **Manage ARP Tables**.

Figure 10-6 displays the Manage ARP Tables menu.

See the following pages for more information about the individual menu items:

Viewing System ARP Entries	10-14
Adding a System ARP Entry	10-14
Deleting a System ARP Entry	10-15
Viewing Adapter ARP Entries	10-15
Adding an Adapter ARP Entry	10-15
Deleting an Adapter ARP Entry with Hardware Address	10-16
Deleting an Adapter ARP Entry with Host Name	10-17
Clearing the Adapter ARP Table	10-17

You can invoke these tasks using command primitives. See "Address Resolution Protocol: Adapter Command Primitives" on page 8-12 and "Address Resolution Protocol: System Command Primitives" on page 8-16 for information about the command primitives.

Viewing System ARP Entries

To view system ARP entries using the System Manager:

1. Select **Resource Control and Management** from the main menu.
2. Select **Manage ARP Tables** from the next menu screen.
3. Select **View System ARP Entries** from the next menu screen.
4. You receive a command status screen displaying a copy of all of the current entries in the system ARP table.

The format for the table entries is as follows:

hostname (IP address) at HWaddress [HWtype]

An example of an ARP table is shown below:

```
666.8 at 10:0:5a:a8:a5:5 [802.3] permanent timer: 0
444.4 at 11:0:6a:a7:11:3 [802.3] permanent timer: 0
```

Adding a System ARP Entry

To add a system ARP entry using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Resource Control and Management** from the main menu.
3. Select **Manage ARP Tables** from the next menu screen.
4. Select **Add System ARP Entry** from the next menu screen.
5. Type in the following information on the dialog screen and press **Enter**:

Hardware type Specify the type of hardware address given. The choices are as follows:

- Ethernet interface
- 802.3 interface
- Token-Ring interface.

Host name (IP Address)

Specify the remote host being added. If the host name is not known, you can use its IP address. The format for an IP address is *nnn.nnn.nnn.nnn* where *nnn* can be any decimal number from 1 to 255.

Hardware address

Specify the address of the adapter in use by the host name given. The format for a hardware address is *nn:nn:nn:nn:nn:nn* where *nn* can be any hexadecimal number from X'0' to X'FF'.

Is this a temporary or permanent entry?

Specify whether the system ARP table entry is permanent or temporary. Temporary entries disappear after a re-IPL of the system.

Do you want to publish this entry?

Specify whether this IBM 6611 system should act as an ARP server and respond to requests for the host name being added, even though the host address does not exist on this particular IBM 6611. This IBM 6611 responds to translation requests for the host name, if the entry is published.

6. You receive a command status screen displaying a message specifying the added entry. For example:

Entry lorax (17.17.17.3) was added to the system ARP table.

Deleting a System ARP Entry

To delete the entry associated with the specified host from the system ARP table using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Resource Control and Management** from the main menu.
3. Select **Manage ARP Tables** from the next menu screen.
4. Select **Delete System ARP Entry** from the next menu screen.
5. Specify the host name of the entry to be deleted on the dialog screen and press **Enter**. You can use the IP address of the remote host, if the host name is not known. The format for an IP address is *nnn.nnn.nnn.nnn* where *nnn* can be any decimal number from 1 to 255.
6. You receive a command status screen displaying a message specifying the deleted entry. For example:

Entry lorax (17.17.17.3) was deleted from system ARP table.

Viewing Adapter ARP Entries

To view adapter ARP entries using the System Manager:

1. Select **Resource Control and Management** from the main menu.
2. Select **Manage ARP Tables** from the next menu screen.
3. Select **View Adapter ARP Entries** from the next menu screen.
4. Select the adapter interface name from the selector screen that appears. See Table 10-1 on page 10-8 for an explanation of the interface name used to identify the adapters. Select either a token-ring or Ethernet interface.
5. You receive a command status screen displaying a copy of all the current entries in the adapter ARP table. The format for the table entries is as follows:
hostname (IP address) at HWaddress [HWtype]

An example of an adapter ARP table is shown below.

ARP Table:

jack (36.24.36.2) at 10:0:5a:c8:0:5a [802.5/SNAP]

Adding an Adapter ARP Entry

To add an adapter ARP entry using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Resource Control and Management** from the main menu.
3. Select **Manage ARP Tables** from the next menu screen.
4. Select **Add Adapter ARP Entry** from the next menu screen.
5. Select the adapter interface name from the selector screen that appears. See Table 10-1 on page 10-8 for an explanation of the interface name used to identify the adapters. Select either a token-ring or Ethernet interface.

6. Supply the following information on the dialog screen and press **Enter**:

Host name (IP address)

Specify the remote host being added. If the host name is not known, you can use its IP address. The format for an IP address is *nnn.nnn.nnn.nnn* where *nnn* can be any decimal number from 1 to 255.

Hardware address

Specify the address of the adapter in use by the host name given. The format for a hardware address is *nn:nn:nn:nn:nn:nn* where *nn* can be any hexadecimal number from X'0' to X'FF'.

Is this a temporary or permanent entry?

Specify whether the adapter ARP table entry is permanent or temporary. Temporary entries disappear after a re-IPL of the system.

Do you want to publish this entry?

Specify whether this IBM 6611 system should act as an ARP server and respond to requests for the host name being added, even though the host address does not exist on this particular IBM 6611. This IBM 6611 responds to translation requests for the host name, if the entry is published.

An entry is created in the adapter ARP table for the specified host and associated adapter address of the network interface chosen. The following is an example of the message displayed on the command status screen.

glc (17.17.17.1) at 10:0:5a:a5:b7:42 added

Deleting an Adapter ARP Entry with Hardware Address

To delete an adapter ARP entry with a hardware address using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Resource Control and Management** from the main menu.
3. Select **Manage ARP Tables** from the next menu screen.
4. Select **Delete Adapter ARP Entry With Hardware Address** from the next menu screen.
5. Select the adapter interface name from the selector screen that appears. See Table 10-1 on page 10-8 for an explanation of the interface name used to identify the adapters. Select either a token-ring or Ethernet interface.
6. Specify the hardware address of the entry to be deleted on the dialog screen and press **Enter**. The format for a hardware address is *nn:nn:nn:nn:nn:nn* where *nn* can be any hexadecimal number from X'0' to X'FF'.

The entry in the adapter interface ARP table is deleted for the specified hardware address. The following is an example of the message displayed on the command status screen:

10:0:5a:c8:0:5a (36.24.36.2) deleted

Deleting an Adapter ARP Entry with Host Name

To delete an adapter ARP entry with a host name using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Resource Control and Management** from the main menu.
3. Select **Manage Route Tables** from the next menu screen.
4. Select **Delete Adapter ARP Entry With Host Name** from the next menu screen.
5. Select the adapter interface name from the selector screen that appears. See Table 10-1 on page 10-8 for an explanation of the interface name used to identify the adapters. Select either a token-ring or Ethernet interface.
6. Specify the remote host name of the entry to be deleted on the dialog screen and press **Enter**. You can use the IP address of the remote host, if the host name is not known. The format for an IP address is *nnn.nnn.nnn.nnn* where *nnn* can be any decimal number from 1 to 255.

The entry in the adapter interface ARP table is deleted for the specified host name or IP address. The following is an example of the message displayed on the command status screen:

jack (36.24.36.2) deleted

Clearing the Adapter ARP Table

This function clears out the adapter ARP table for a specific network interface.

To clear an adapter ARP table using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Resource Control and Management** from the main menu.
3. Select **Manage ARP Tables** from the next menu screen.
4. Select **Clear Adapter ARP Table** from the next menu screen.
5. Select the adapter interface name from the selector screen that appears. See Table 10-1 on page 10-8 for an explanation of the interface name used to identify the adapters. Select either a token-ring or Ethernet interface.

The command status screen displays a message stating that the ARP table for the specified adapter is cleared.

Viewing Adapter AARP Entries

To view adapter AppleTalk Address Resolution Protocol (AARP) entries using the System Manager:

1. Select **Resource Control and Management** from the main menu.
2. Select **View Adapter AARP Entries** from the next menu screen.
3. Select the adapter interface name from the selector panel that appears. See Table 10-1 on page 10-8 for an explanation of the interface name used to identify the adapters. Select either a token-ring or Ethernet interface.
4. You receive a command status screen displaying a copy of all of the current entries in each of the interface's AARP table.

The format for the table entries is as follows:

network_number.nodeID at HWaddress [HWtype] Status EntryAge

- The HWtypes include [802.3] Ethernet, [802.5] token-ring, and [T1] serial interfaces.
- The ARP status indicators are In_Use, Permanent, Need_ARP, Did_ARP, and New_Entry.
- The EntryAge is represented in seconds, where the low values represents recently used entries and high timer values represent old entries.

An example of an ARP table is shown below:

```
666.8 at 10:0:5a:a8:a5:5 [802.3] permanent timer: 0
444.4 at 11:0:6a:a7:11:3 [802.3] permanent timer: 0
```

Exporting the Route Table Information

To export the route table using the System Manager:

1. Select **Resource Control and Management** from the main menu.
2. Select **Export Route Information** from the next menu.
3. Select an Export method from the selector screen.
 - FTP
 - Modem
 - DOS diskette
 - UNIX diskette.
4. With each of these file transfer methods, a selector screen appears requesting the name of the file to be transferred. Select the name of the route table file.
 - Transferring files with FTP requires you to give the host name and a userid at the destination node on the dialog screen. You are prompted for the password for the userid.
 - Transferring files to a DOS diskette requires you to give the name of the file on the DOS diskette.
 - Transferring files to a UNIX diskette requires you to specify whether to *append* the file to the end of the diskette or to place it as the only file on the diskette, *create*.

Figure 10-7 shows an example of the message you receive after exporting the system route table to a UNIX diskette.

The file system.routes has been placed on a UNIX diskette occupying 2 blocks.

Figure 10-7. Example of Export Route Information to UNIX Diskette

Performing System Environment and Configuration Tasks

The System Environment and Configuration menu allows you to perform several operational tasks to set up the IBM 6611. Figure 10-8 on page 10-19 displays the System Environment and Configuration menu.

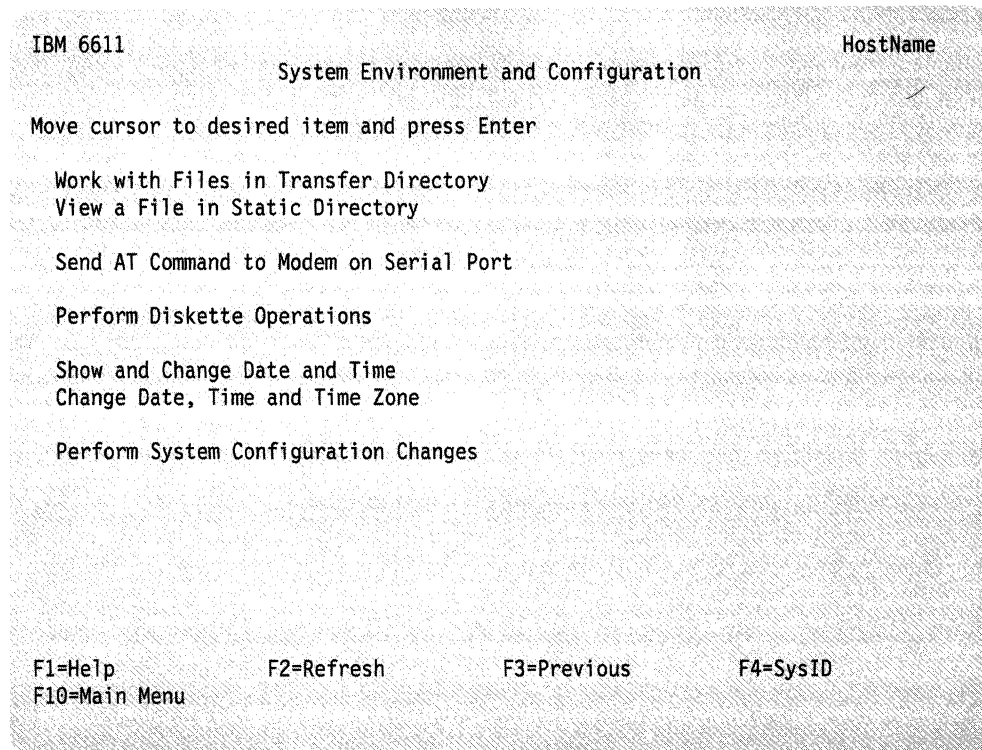


Figure 10-8. System Environment and Configuration Screen

See the following pages for more information about the individual menu items:

Working with Files in the Transfer Directory	10-19
Viewing a File in the Static Directory	10-21
Sending an AT Command to a Modem Attached to an EIA 232 Serial Port	10-22
Performing Diskette Operations	10-22
Showing and Changing the Date and Time	10-26
Changing the Date, Time, and Time Zone	10-27
Performing System Configuration Changes	10-28

Working with Files in the Transfer Directory

A file transferred into the IBM 6611 is placed in the *transfer directory*. A file, that needs to be transferred out of the IBM 6611, must be in either the *transfer directory* or the *static directory*.

You can view, rename, delete and transfer the files in the transfer directory. Only a controlling user can rename or delete files in the transfer directory. The static directory holds special files placed there by system components that allow the files to be viewed or transferred out of the IBM 6611, but do not allow them to be deleted or renamed.

Most of the files in the transfer directory are placed there because you selected the **transfer_directory** as the destination when executing a System Manager function. Please delete unneeded files in a timely manner to prevent the transfer directory from becoming full.

A few files in the transfer directory are trace logs that can grow. Most of these are not started by System Manager commands. Do not erase these files, unless you are instructed to do so by IBM service personnel.

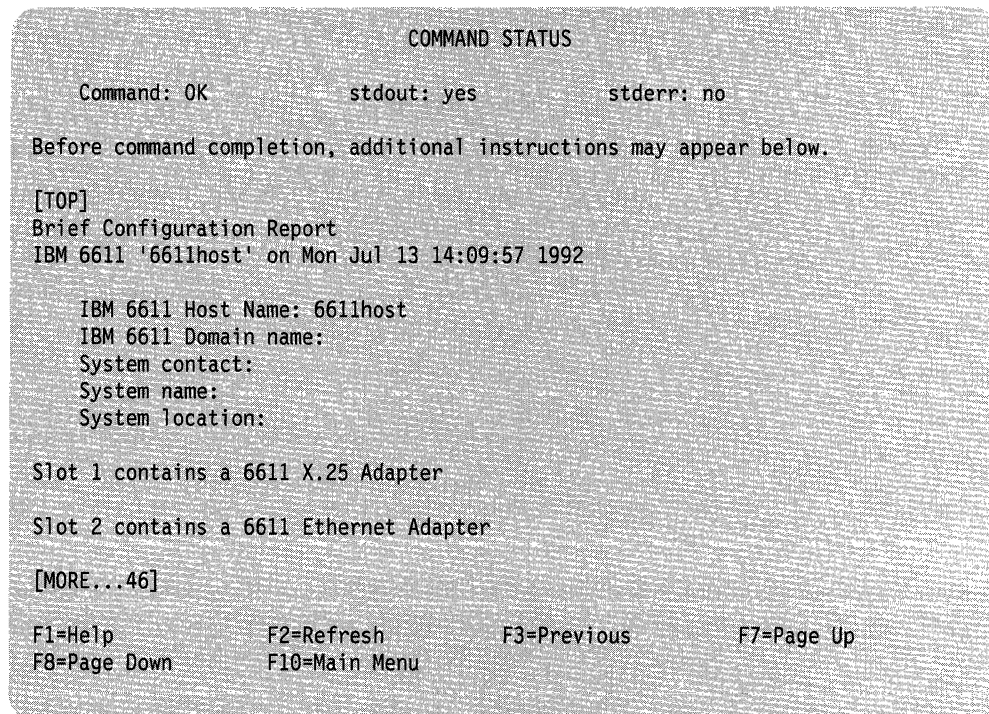


Figure 10-9. Viewing a Transfer Directory File

If you notice some files in the transfer directory which are not listed in the following tables, contact the IBM service personnel.

There is a detailed discussion about the transfer directory files in "File Names for Output in Transfer Directory" on page 10-43. If you notice some files in the transfer directory which are not listed in the tables in this section, contact IBM service personnel.

To work with files in the transfer directory using the System Manager:

1. Select **System Environment and Configuration** from the main menu.
2. Select **Work with Files in Transfer Directory** from the next menu.
3. Select the action to be performed on the file from the selector screen. You can perform these actions:
 - View
 - Rename
 - Delete.

Go to 4, if you want to **view** a file.

Go to 7, if you want to **rename** a file.

Go to 11, if you want to **delete** a file.

4. **View** allows you to view the contents of a selected file in the transfer directory.
5. Select the file to view on the selector screen. At the top of the screen the amount of space available in the transfer directory is displayed.
6. A command status screen displays the contents of the file you selected to view. See Figure 10-9 for an example of viewing a brief configuration report in the transfer directory.

7. *Rename* allows you to rename any file in the transfer directory.
8. Select the file to rename on the selector screen.
9. Enter the new name of the file on the dialog screen.
10. A command status screen displays the following message:
File, `old_file_name`, in the transfer directory has been renamed to `new_file_name`.
11. *Delete* allows you to delete a file from the transfer directory.
12. Select the files to delete on the selector screen. Press **F9 (Esc + 9)** to select the files to delete. Press **Enter** to register the selections.
A command status screen displays the following message:
Files `file_name` deleted from the transfer directory

You can invoke these tasks using command primitives. See “File Management Command Primitives” on page 8-54 for information about the command primitives. If you need to transfer files to or from the transfer directory, see “Transferring Files” on page 10-43.

Viewing a File in the Static Directory

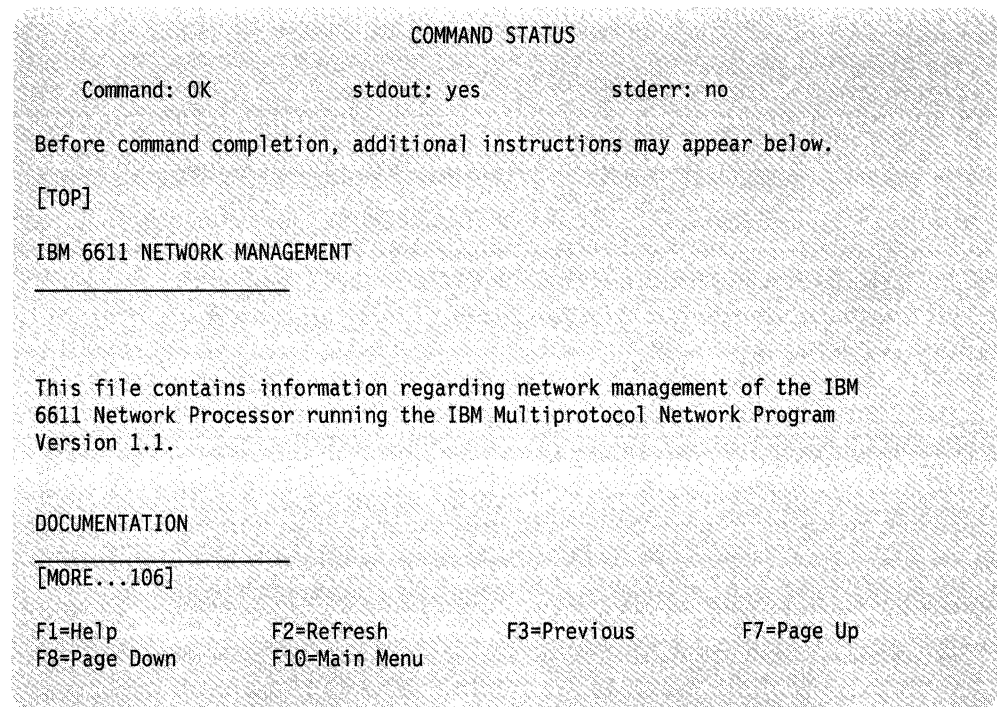


Figure 10-10. Viewing a Static Directory File

A file, that needs to be transferred out of the IBM 6611, must be in either the *transfer directory* or the *static directory*. You can view, rename, delete and transfer the files in the transfer directory. The static directory holds special files placed there by system components that allow the files to be viewed or transferred out of the IBM 6611, but do not allow them to be deleted or renamed.

To view files in the static directory:

1. Select **System Environment and Configuration** from the main menu.

2. Select **View a File in Static Directory** from the next menu. A selector screen appears listing all of the files in the static directory.
3. Select the file name that you want to view.

A command status screen displays the contents of the file you selected to view. See Figure 10-10 on page 10-21 for an example of viewing a file from the static directory.

You can invoke this task using command primitives. See “File Management Command Primitives” on page 8-54 for information about the command primitives. If you need to transfer a file out of the static directory, see “Transferring Files” on page 10-43.

Sending an AT Command to a Modem Attached to an EIA 232 Serial Port

The IBM 6611 supports modem configuration using the AT command set. The Attention (AT) Command Set is a group of modem commands that allow the IBM 6611 to control the modem while it is operating in asynchronous mode. The modem accepts an AT command using the AT sequence followed by one or more commands, command parameters if any, and a carriage return. Refer to the manufacturer’s documentation for the modem you are using for more information. The System Manager allows you to send multiple AT commands to a modem.

To configure a modem using the System Manager:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** from the main menu.
3. Select **Send AT Command to Modem on Serial Port** from the next menu. A selector screen is displayed.
4. Select the EIA 232 serial port to which you want to send the AT command. The choices are **S1** or **S2**.
5. Answer the prompts and enter the AT commands when prompted. For example:

Prompt: Initializing the port (takes about 20 secs)...
Ready to enter AT commands ? (y or n)

Type Answer: y

Prompt: Enter AT command

Type Answer: ATZ 123

Prompt: More AT commands ? (y or n)

Type Answer: n

Message: Closing the port (takes about 16 secs).

You can invoke this task using a command primitive. See “Serial Port Command Primitives” on page 8-74 for information about the command primitives.

Performing Diskette Operations

There are four general diskette operations that can be performed from the System Manager:

- Format a diskette
- List files on diskette
- Import files from diskette
- Export files to diskette.

You can use UNIX and DOS diskettes. To work with a UNIX or DOS diskette:

1. Select **System Environment and Configuration** from the main menu.
2. Select **Perform Diskette Operations** from the next menu. Figure 10-11 shows the items on the Perform Diskette Operations menu.

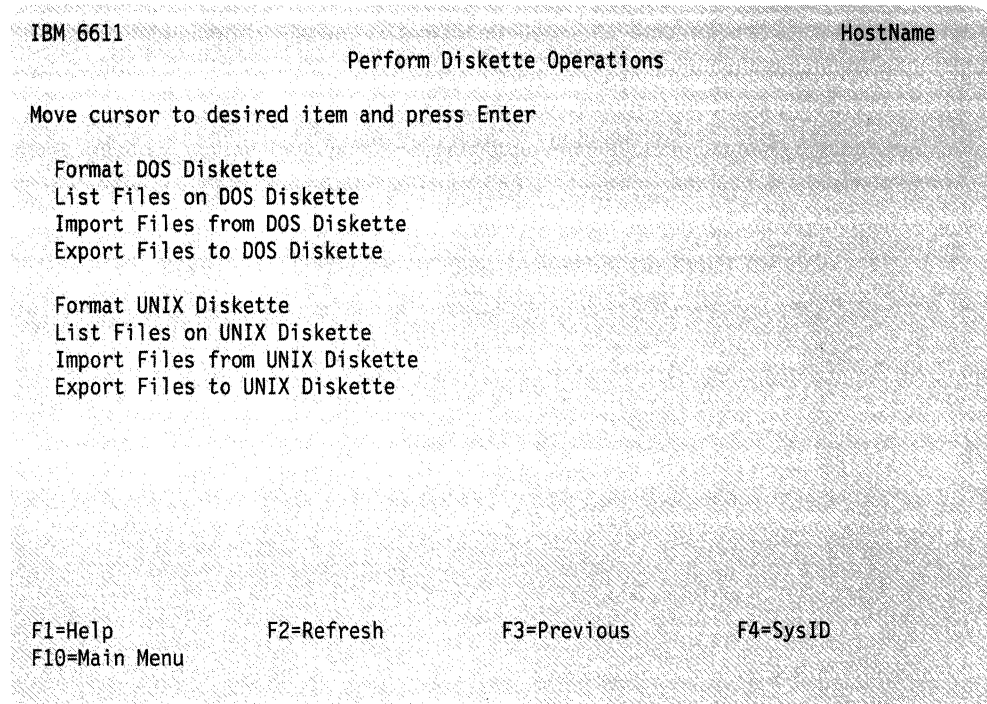


Figure 10-11. Performing Diskette Operations Menu

See the following pages for more information about the individual menu items:

Formatting a DOS or UNIX Diskette	10-23
Listing Files on a DOS or UNIX Diskette	10-24
Importing Files From a DOS or UNIX Diskette	10-24
Exporting Files to a DOS or UNIX Diskette	10-25

You can invoke these tasks using command primitives. See “Diskette Command Primitives” on page 8-37 for information about the command primitives.

Formatting a DOS or UNIX Diskette

To format a DOS or UNIX diskette:

1. Place the diskette in the IBM 6611 diskette drive.
2. Select **Format DOS Diskette** or **Format UNIX Diskette** from the Perform Diskette Operations menu.
3. Select the diskette density for the diskette from the selector screen. The choices are **high** and **low**.
4. An information message screen displays requesting you to confirm your decision to format the diskette.

With Format DOS Diskette the following message appears on the command status screen when the formatting completes:

```
Formatting ... Format Complete
1457664 bytes total disk space
1457664 bytes available on disk
Format another (Y/N)?
```

Answer either **Y** or **N**.

With Format UNIX Diskette the following message appears on the command status screen when the formatting completes:

```
Formatting UNIX Diskette
Press Ctrl+C to stop
Formatting: 2 side(s), 80 trl/side, 18 sect/trk
Format completed
Completed formatting UNIX diskette
```

Listing Files on a DOS or UNIX Diskette

To list the files on a DOS or UNIX diskette:

1. Place the diskette in the IBM 6611 diskette drive.
2. Select **List Files on DOS Diskette** or **List Files on UNIX Diskette** from the Perform Diskette Operations menu.

A command status screen displays the files on the diskette.

For example, with List Files on DOS Diskette you receive:

```
SCM_CONF.RPT
CONFIG
PS.STA
VPD.LST
PD_ERROR.LOG
CONF.SH
TRBUG1.ERR
TRBUG7.ERR
SCM.RPT
IOSTAT.TXT
Free space: 680960 bytes
```

For example, with List Files on UNIX Diskette you receive:

```
-rw-rw-rw-  0 0      734 Apr 23 18:06:20 1992 ps_io.stat
-rw-rw-rw-  0 0     1124 Apr 23 18:06:22 1992 ps_vm.stat
```

Importing Files From a DOS or UNIX Diskette

To place the files from a DOS or UNIX diskette into the transfer directory:

Note: The files cannot be sent to the static directory.

1. Place the diskette in the IBM 6611 diskette drive.
2. Select **Import Files from DOS Diskette** or **Import Files from UNIX Diskette** from the Perform Diskette Operations menu.
3. Select the file or files to import from the dialog screen. Press **F4 (Esc + 4)** to list the files on the diskette.

For Import Files from DOS Diskette you can only choose one file. Press **Enter** on the file name to select it. Enter the name of the files as it should appear in the transfer directory.

For Import Files from UNIX Diskette press **F9 (Esc + 9)** to select multiple files. Press **Enter** to record the selections. A message appears describing the completed operation.

For Import Files from DOS Diskette the completion message is:

DOS file old_name has been loaded into new_name.
new_name is placed in the transfer directory.

For Import Files from UNIX Diskette the completion message is:

The loading of files from the UNIX diskette is complete.
The files loaded are placed in the transfer directory.

Exporting Files to a DOS or UNIX Diskette

This menu item sends files from the transfer or static directories to a DOS or UNIX diskette.

To place the files on a diskette:

1. Place the diskette in the IBM 6611 diskette drive.
2. Select **Export Files to DOS Diskette** or **Export Files to UNIX Diskette** from the Perform Diskette Operations menu.
3. Select the directory that contains the files to be exported from the selector screen. The choices are the **transfer directory** or **static directory**.
4. Select the file or files to export on the dialog screen. Press **F4 (Esc + 4)** to list the files in the selected directory. Press **Enter** to record the selections.

For Export Files to DOS Diskette enter the name of the file as it should appear on the diskette.

For Export Files to UNIX Diskette select the archive type of either **append** or **create**. If the file is to be placed on a diskette with existing files, select **append**. If the file is the first to be placed on the diskette, select **create**.

5. A message appears describing the completed operation.

For Export Files to DOS Diskette the completion message is:

File new_name has been exported to DOS diskette.

For Import Files from UNIX Diskette the completion message is:

The files are being exported to the UNIX diskette.
The exporting of files to the UNIX diskette has completed.

Diskette Operations on a Model 170 With 7 Peer-Capable Adapters

When all seven slots in an IBM 6611 Model 170 contain peer-capable adapters (EIA 422/449 Serial Adapter, V.35/V.36 Serial Adapter, Ethernet Adapter, or Token-Ring Network 16/4 Adapter) in any combination, the system disables the diskette drive after the IBM 6611 is started.

If you want to transfer files to or from diskettes, IBM recommends two ways to perform diskette operations:

- Attach a workstation capable of diskette operations to one of the EIA 232 serial ports. You can only use DOS formatted diskettes with this process.
- Reconfigure the Model 170 to enable the diskette drive.

Attaching a Workstation Capable of Diskette Operations to a EIA 232 Serial Port:

For a direct-attached workstation, use the following setup to attach a workstation with a terminal emulator program to one of the EIA 232 serial ports, labelled S1 and S2 on the Model 120 and Model 170, and labelled Serial 1 and Serial 2 on the Model 140. The workstation must be able to perform diskette operations.

1. You should initially set the terminal emulator program and the EIA 232 serial port to operate at the highest baud rate possible (typically 19200 bps or 38400 bps). This maximizes the performance of any data transfers invoked. Set the baud rate of the EIA 232 serial port on the Model 170 using the System Manager. See "Configuring the EIA 232 S1 and S2 Serial Ports" on page 10-30. If possible, do not change the baud rate from a terminal that has accessed the System Manager over the same serial port for which the baud rate is being changed. If you do this, it will terminate your System Manager session. You will need to restart your System Manager session after you have matched the baud rates.
2. Set the baud rate of the terminal emulator program to match the baud rate of the EIA 232 serial port.
3. When using a terminal emulator program, ensure that the connection is set to **direct connect** (not modem connect).
4. Restart the System Manager session.
5. Even though this is a direct connection, you need Xmodem to transfer the files between the IBM 6611 and the workstation. To send a file, use the Send Files to Another Node menu item. To receive a file, use the Receive Files from Another Node menu item. Select **modem** from the "Transfer method" selector screen. See "Using the Xmodem Protocol" on page 10-55 for more information.

Note: You cannot import software updates using these procedures because the updates are not generated in DOS format.

Reconfiguring the Model 170 to Enable the Diskette Drive: The following procedure allows you to use the diskette drive on a Model 170:

1. Prepare a secondary configuration that enables fewer than 7 peer-capable adapters using the Configuration Program.
2. Shut down the Model 170. See "Stopping the IBM 6611" on page 10-4 for more information.
3. Power off the Model 170.
4. Place the secondary configuration diskette in the diskette drive.
5. Power on the Model 170.
6. Log in to the IBM 6611 and use the System Manager to perform the diskette operations.
7. When you are finished using the diskette drive, shut down the Model 170. See "Stopping the IBM 6611" on page 10-4 for more information.
8. Power off the Model 170.
9. Restore the Model 170 using the primary configuration diskette and turn the power on.

Showing and Changing the Date and Time

You can change the date and time from this menu item or just display the current time. When changing the date and time, the changes do not become effective for any user until they log out and log back into the IBM 6611.

To change the date and time:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** from the main menu.

3. Select **Show and Change Date and Time** from the next menu.
4. On the dialog screen, enter the new time and date if you want to change it. Otherwise, just press Enter to display the current date and time. The accepted values are as follows:

Year	00 – 99
Month	01 – 12
Day	01 – 31
Hour	00 – 23
Minutes	00 – 59
Seconds	00 – 59

A command status screen appears with the new date and time. For example:

Fri Apr 24 09:30:20 1992

You can invoke this task using a command primitive. See “Time: System Command Primitives” on page 8-89 for information about the command primitive.

Changing the Date, Time, and Time Zone

When changing the date, time, and time zone, the changes do not become effective for any user until they log out and log back into the IBM 6611.

To change the date, time, and time zone:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** from the main menu.
3. Select **Change Date, Time, and Time Zone** from the next menu.
4. Answer daylight savings time question from the selector screen. Select **yes** if the time zone goes on daylight savings time, or **no** if it does not.
5. Select the correct time zone from the next selector screen.
6. On the dialog screen, enter the new time and date. The accepted values are as follows:

Year	00 – 99
Month	01 – 12
Day	01 – 31
Hour	00 – 23
Minutes	00 – 59
Seconds	00 – 59

A command status screen appears with the new date and time and a message. For example:

Fri Apr 24 09:30:20 1992

Now exit System Manager and then re-enter so that any changes to date, time, and time zone will be reflected in your current session.

You can invoke this task using a command primitive. See “Time: System Command Primitives” on page 8-89 for information about the command primitive.

Performing System Configuration Changes

You can make changes to the system configuration using the Perform System Configuration Changes menu. This menu is shown in Figure 10-13 on page 10-30. All of these tasks can also be performed using the Configuration Program and with the Adapter and Protocol Configuration screens.

Only a controlling user can use the System Manager to update configuration parameters.

The System Manager method of configuring the IBM 6611 includes an apply, test, and either commit or reject scenario. The configuration changes are *applied* and *tested* in an actual test environment, and then either *committed* if the changes are approved, or *rejected* if the changes are not approved. Refer to “Configuration Procedure” on page 14-8 for the details of this scenario.

When you begin modifying the system configuration using the System Manager, a local copy of the configuration data is created in the home directory of your userid, which acts as a work file in which any additional configuration modifications are recorded. These changes are not yet part of the system configuration database.

If you want to try out the changes, but want to be able to restore the original configuration, Apply Changes to Configuration Database may be selected from the Perform System Configuration Changes menu. This will cause the current configuration to be saved in the home directory of your userid, before the configuration changes from the work file are made a part of the current configuration. At some time later you can decide to commit these changes. You may make additional modifications to the configuration, and apply these changes in an incremental fashion.

If you are satisfied with the changes and want to commit them to the configuration database, selecting Commit Changes to Configuration Database will give you the choice of committing only the previously applied changes or both the previously applied changes and the unapplied changes made from this userid. The System Manager will then make the configuration changes described in the work file a permanent part of the current configuration.

If you want to remove uncommitted configuration changes, selecting Reject Uncommitted Changes to Configuration Database will give you the choice of undoing all your configuration changes since the last commit operation, (both applied and unapplied changes), or to simply discard any changes made since the last apply or commit operation (only unapplied changes).

When you begin to modify the configuration data from a specific userid and a local copy is made, the System Manager will display the modified version, not the current version. Since the local copy is user-specific, changes that have not been applied or committed will only be seen using that particular userid. When the changes have been committed or applied, the System Manager will return to showing the current configuration. This may be confusing if multiple users are modifying or importing configuration data.

You can view the status of your configuration changes by pressing F4 or Esc + 4, from any System Manager menu screen. An example of this screen is shown in Figure 10-12 on page 10-29. When viewing this screen, press **Enter** to return to the System Manager menu screen.

When the System Manager is used to create the latest applied or committed configuration changes, the configuration name has the following format:

localhost(userid) Date Time

The *userid* is the user name that was used to create the latest applied or committed configuration changes.

The configuration status is either **current**, **applied**, **unapplied**, or **partially applied**.

If the status is **current**, then all configuration changes made from the userid that you are logged into have been committed. However, there may be unapplied or applied configuration changes created from a different userid. If the configuration name has the localhost format, check the userid field to determine the last user who updated the configuration.

If the status is **applied**, then the userid that you are logged into has some applied, but not committed configuration changes.

If the status is **unapplied**, then the userid that you are logged into has some unapplied configuration changes.

If the status is **partially applied**, then the userid that you are logged into has some applied and unapplied configuration changes.

If you want to view only the applied or committed changes, log off and log back in with another userid. The configuration output produced from the different userid will not reflect the unapplied changes made from the previous userid. It will reflect all applied changes made from the previous userid.

Warning: Make all System Manager configuration changes from the same controlling userid to minimize the possibility of overriding another user's configuration changes.

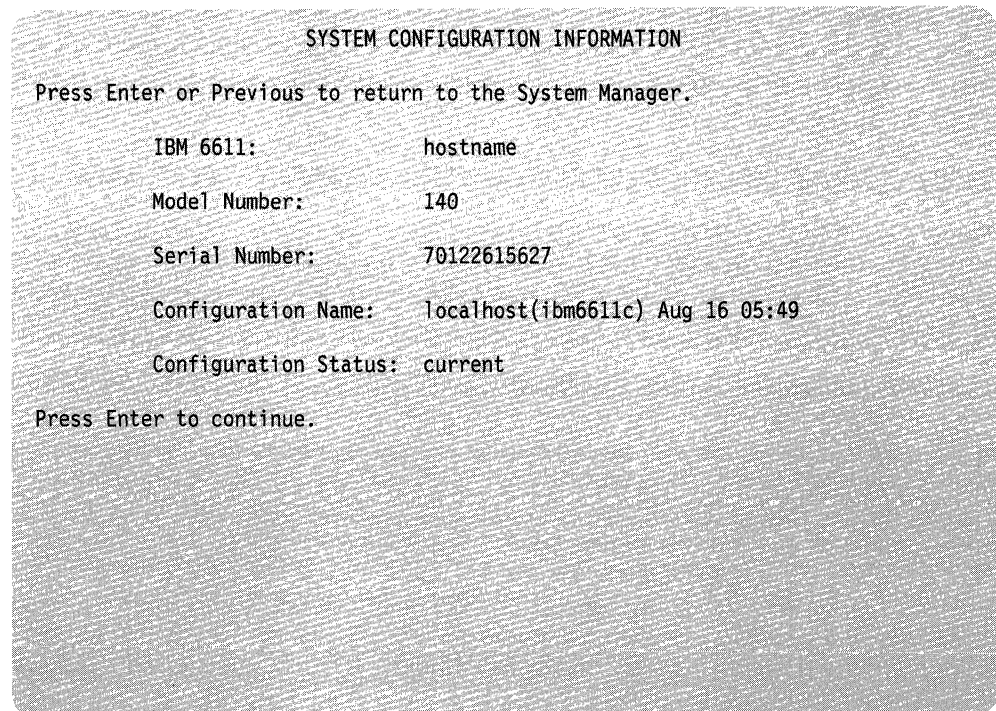


Figure 10-12. System Configuration Information Screen

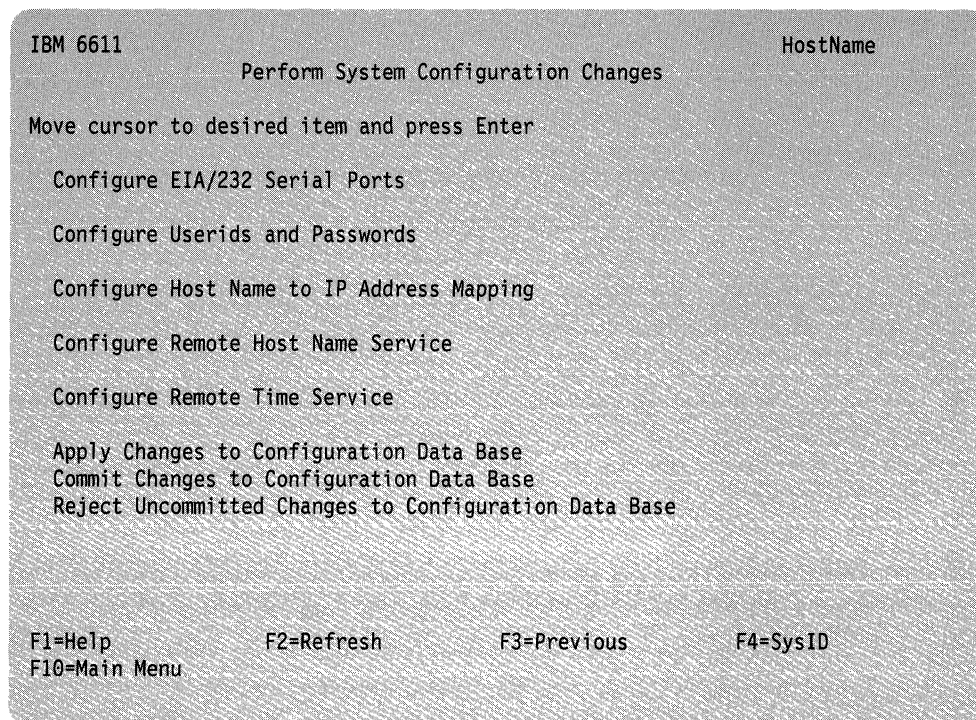


Figure 10-13. Perform System Configuration Changes Menu

See the following pages for more information about the individual menu items:

Configuring the EIA 232 S1 and S2 Serial Ports	10-30
Configuring Userids and Passwords	10-31
Configuring Host Name to IP Address Mapping	10-34
Configuring Remote Host Name Service	10-37
Configuring Remote Time Service	10-39
Apply Changes to Configuration Database	10-41
Commit Changes to Configuration Database	10-42
Reject Uncommitted Changes to Configuration Database	10-42

Configuring the EIA 232 S1 and S2 Serial Ports

The S1 and S2 serial ports are used to attach a service terminal either directly or through a modem. When managing a Cylink CSU/DSU via its EIA 232 port, S2 must be used and the S2 baud rate must match the baud rate that is configured on the Cylink DSU/CSU. The line speed or baud rate is the only parameter that you can change on these ports. Five baud rates are supported:

- 1200 bps
- 2400 bps
- 9600 bps
- 19200 bps
- 38400 bps.

A baud rate of 9600 is normal for a direct-attached terminal. A baud rate of 2400 should be set for a modem-attached terminal. The higher baud rates, 19200 and 38400 bps are useful when a PC terminal emulator is direct-attached and used for its diskette capabilities. See "Diskette Operations on a Model 170 With 7

Peer-Capable Adapters” on page 10-25 for information about the scenario when this should be considered.

The S1 serial port is initially configured for a direct connection with a baud rate of 9600 bps. You need to reconfigure the port if you want to change the baud rate.

To configure the EIA 232 S1 or S2 serial ports:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** from the main menu.
3. Select **Perform System Configuration Changes** from the next menu.
4. Select **Configure EIA/232 Serial Ports** from the next screen.
5. On the selector screen, select **modem** if you are configuring the serial port for a remote switched connection. Select **direct** if you are configuring the serial port for a direct-attached terminal.
6. On the next selector screen, select **S1** if you are configuring the S1 serial port. Select **S2** if you are configuring the S2 serial port.
7. Select the baud rate from the dialog screen. Press **Tab** to cycle through the baud rates.

A command status screen displays the following message:

Command completed successfully.
S2 baud rate changed to 9600.

8. Press **F3 (Esc + 3)** to back up to the Perform System Configuration Changes menu and select **Apply Changes to Configuration Database** to apply the configuration change.

Note: The baud rate for a EIA 232 serial port should not be changed from a direct-attached terminal or a modem-attached terminal that has accessed the System Manager over the same serial port for which the baud rate is being changed. If you do this, it will terminate your System Manager session. You will need to restart your System Manager session after you have matched the baud rates.

You can invoke this task using command primitives. See “Serial Port Command Primitives” on page 8-74 for information about the command primitives.

Configuring Userids and Passwords

To log into the IBM 6611 you are required to have a userid and password. There are two classes of users (Refer to “Controlling User Tasks” on page 9-25 for additional information):

- Controlling
- Viewing.

Users with viewing privileges cannot perform all the operations of the IBM 6611. Full privileges are given to the controlling class. You can configure multiple controlling and viewing users. Up to 10 users can be logged into the IBM 6611, simultaneously. However, IBM recommends that you allow up to 5 users at one time to improve system performance.

Two default userids are configured with the IBM 6611, one controlling and one viewing. The controlling userid and password is ibm6611c. The viewing userid and password is ibm6611v. IBM recommends that you delete these userids or change the passwords shortly after receiving the IBM 6611. The default userids are to be used during initial configuration of the IBM 6611, if performed using the System Manager.

From the System Manager you can list all the users, add a user, delete a user and change user passwords. Only a controlling user can change or add userids or passwords. The only exception is the ability of any user to change their own password. When adding or deleting system users, the configuration change must be applied or committed before it becomes part of the base configuration. The apply is done automatically, when a user changes his own password.

To configure userids and passwords:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** from the System Manager main menu.
3. Select **Perform System Configuration Changes** from the next menu.
4. Select **Configure Userids and Passwords** from the next menu.
5. Figure 10-14 shows the Configure Userids and Passwords menu.

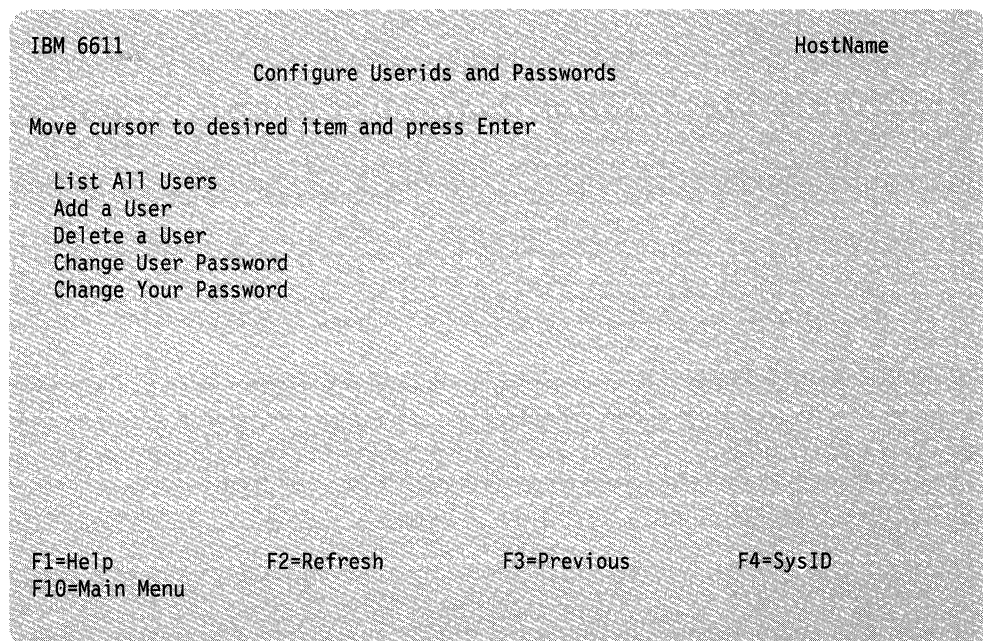


Figure 10-14. Configure Userids and Passwords Menu

See the following pages for more information about the individual menu items:

List All Users	10-33
Add a User	10-33
Delete a User	10-33
Change User Password	10-34
Change Your Password	10-34

You can invoke these tasks using command primitives. See "User: System Command Primitives" on page 8-98 for information about the command primitives.

List All Users: To list system users:

1. Select **System Environment and Configuration** from the System Manager main menu.
2. Select **Perform System Configuration Changes** from the next menu.
3. Select **Configure Userids and Passwords** from the next menu.
4. Select **List All Users** from the next menu.

A command screen displays all of the configured controlling and viewing userids. For example,

Controlling users:
ibm6611c

Viewing users:
ibm6611v

Add a User: To add a system user:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** from the System Manager main menu.
3. Select **Perform System Configuration Changes** from the next menu.
4. Select **Configure Userids and Passwords** from the next menu.
5. Select **Add a User** from the next menu.
6. Type in the user name and select the privilege class using the **Tab** on the dialog screen. A user name is a unique string of 8 alphanumeric lowercase characters or fewer. The privilege class is either viewing or controlling.
7. You are prompted for the password for the new user. Enter the password twice. It is not displayed. For example:

Enter new password for userid
Enter new password again
Command completed successfully
8. Press **F3 (Esc + 3)** to back up to the Perform System Configuration Changes menu and select **Apply Changes to Configuration Database** to apply the configuration change.

Delete a User: To delete a system user:

1. Log in using a controlling userid.
2. Select **Perform System Configuration Changes** from the next menu.
3. Select **Configure Userids and Passwords** from the next menu.
4. Select **Delete a User** from the next menu.
5. Select the userid to be deleted from the selector screen.

You receive the following message:

Command completed successfully
User userid has been removed from the system

6. Press **F3 (Esc + 3)** to back up to the Perform System Configuration Changes menu and select **Apply Changes to Configuration Database** to apply the configuration change.

Change User Password: To change a user password:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** from the System Manager main menu.
3. Select **Perform System Configuration Changes** from the next menu.
4. Select **Configure Userids and Passwords** from the next menu.
5. Select **Change User Password** from the next menu.
6. Select the userid to be whose password is being changed from the selector screen.
7. You are prompted for the new password for the user. Enter the password twice. It is not displayed. For example:
Enter new password for userid
Enter new password again
Deleting Old password for userid; please be patient
Old password for userid has been deleted
Adding new record for userid; please be patient
Command completed successfully
Password changed for userid
8. Press **F3 (Esc + 3)** to back up to the Perform System Configuration Changes menu and select **Apply Changes to Configuration Database** to apply the configuration change.

Change Your Password: To change your password:

1. Select **System Environment and Configuration** from the System Manager main menu.
2. Select **Perform System Configuration Changes** from the next menu.
3. Select **Configure Userids and Passwords** from the next menu.
4. Select **Change Your Password** from the next menu.
5. You are prompted for your old and new password. Enter the old password once and the new password twice. They are not displayed. For example:
Enter old password for userid
Enter new password for userid
Enter new password again
Deleting old password for userid; please be patient
Old password for userid has been deleted
Adding new record for userid; please be patient
Command completed successfully
Password changed for userid

Configuring Host Name to IP Address Mapping

Figure 10-15 on page 10-35 shows the Configure Host Name to IP Address Mapping menu. With the first menu item, Set Host Name Information, you can specify the host name and domain name for this IBM 6611. The other three menu items allow you to manage the host names that are mapped to their IP addresses in the IBM 6611.

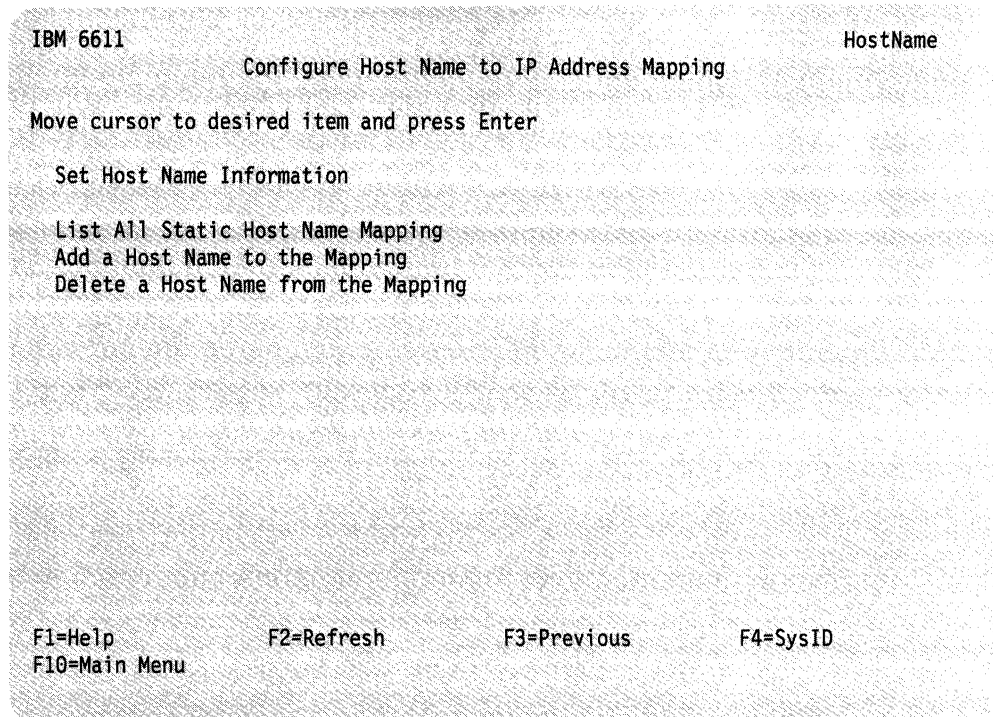


Figure 10-15. Configure Host Name to IP Address Mapping Menu

See the following pages for more information about the individual menu items:

Setting Host Name Information	10-35
Listing All Static Host Name Mappings	10-36
Adding a Host Name to the Mapping	10-36
Deleting a Host Name from the Mapping	10-36

You can invoke these tasks using command primitives. See “Host Name Command Primitives” on page 8-60 and “Host Name to IP Address Mapping Command Primitives” on page 8-61 for information about the command primitives.

Setting Host Name Information: To set the host name and domain name for this IBM 6611 using the System Manager:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** from the main menu.
3. Select **Perform System Configuration Changes** from the next menu.
4. Select **Configure Host Name to IP Address Mapping** from the next menu.
5. Select **Set Host Name Information** from the next menu.
6. On the dialog screen, enter the host name and domain name in the entry fields. You receive a completion message. For example,
 Command completed successfully
 If you exit the System Manager and re-enter, the changed host name should appear in the top right corner of every menu screen.
7. Press **F3 (Esc + 3)** to back up to the Perform System Configuration Changes menu and select **Apply Changes to Configuration Database** to apply the configuration change.

Listing All Static Host Name Mappings: To list all static host name mappings using the System Manager:

1. Select **System Environment and Configuration** from the main menu.
2. Select **Perform System Configuration Changes** from the next menu.
3. Select **Configure Host Name to IP Address Mapping** from the next menu.
4. Select **List All Static Host Name Mappings** from the next menu. You receive a list of the configured hosts and their IP addresses. For example,
IP address of host: 17.17.17.1
Host name: glc

Adding a Host Name to the Mapping: To add a host name and IP address pair to the mapping using the System Manager:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** from the main menu.
3. Select **Perform System Configuration Changes** from the next menu.
4. Select **Configure Host Name to IP Address Mapping** from the next menu.
5. Select **Add a Host Name to the Mapping** from the next menu.
6. Enter the host name and IP address in the appropriate entry fields on the dialog screen. The format for the IP address is *nnn.nnn.nnn.nnn* where *nnn* can be any decimal number from 1 to 255. You receive a completion message. For example,
Command completed successfully
Added glc with an IP Address of 17.17.17.1 to the mapping
7. Press **F3 (Esc + 3)** to back up to the Perform System Configuration Changes menu and select **Apply Changes to Configuration Database** to apply the configuration change.

Deleting a Host Name from the Mapping: To delete a host name from the mapping using the System Manager:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** from the main menu.
3. Select **Perform System Configuration Changes** from the next menu.
4. Select **Configure Host Name to IP Address Mapping** from the next menu.
5. Select the host name for the host name and IP address pair to be deleted from the selector screen. You receive a completion message. For example,
Command completed successfully
Deleted glc with an IP Address of 17.17.17.1 from the mapping
6. Press **F3 (Esc + 3)** to back up to the Perform System Configuration Changes menu and select **Apply Changes to Configuration Database** to apply the configuration change.

Configuring Remote Host Name Service

Remote name service is a mechanism where the IBM 6611 can request to have a host name translated into an IP address by a remote name server. When enabled, this IBM 6611 sends its name request to the first remote name server listed in the list of remote name servers. If the first remote name server listed is unable to provide name service, the request is sent to the second remote name server in the list. Figure 10-16 shows the Configure Remote Host Name Service menu.

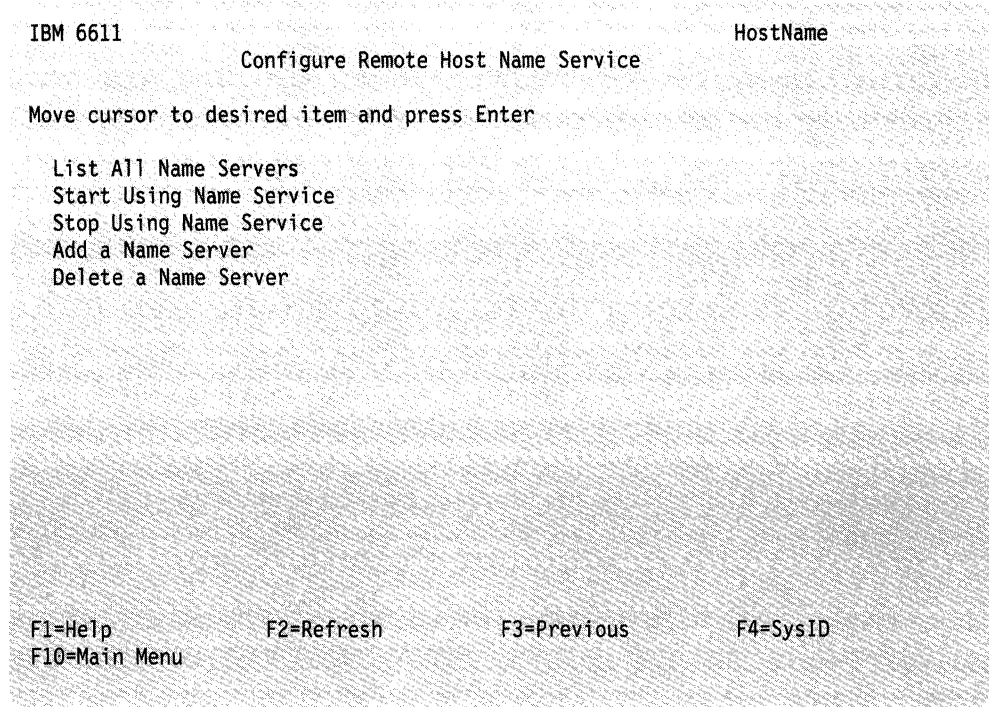


Figure 10-16. Configure Remote Host Name Service Menu

See the following pages for more information about the individual menu items:

Listing All Name Servers	10-37
Start Using the Name Service	10-38
Stop Using the Name Service	10-38
Adding a Name Server	10-38
Deleting a Name Server	10-39

You can invoke these tasks using command primitives. See “Name Server Command Primitives” on page 8-66 for information about the command primitives.

Listing All Name Servers: To list all remote name servers:

1. Select **System Environment and Configuration** from the main menu.
2. Select **Perform System Configuration Changes** from the next menu.
3. Select **Configure Remote Host Name Service** from the next menu.
4. Select **List All Name Servers** from the next menu.

A command status screen displays a listing of the IP addresses of all the name servers. For example,

IP Address of Domain Name Server:
215.1.230.142

Start Using the Name Service: To start using remote name service:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** from the main menu.
3. Select **Perform System Configuration Changes** from the next menu.
4. Select **Configure Remote Host Name Service** from the next menu.
5. Select **Start Using Name Service** from the next menu.

A command status screen displays the following message.

Command completed successfully

Domain Name Service is enabled

6. Press **F3 (Esc + 3)** to back up to the Perform System Configuration Changes menu and select **Apply Changes to Configuration Database** to apply the configuration change.

Stop Using the Name Service: To stop using name service:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** from the main menu.
3. Select **Perform System Configuration Changes** from the next menu.
4. Select **Configure Remote Host Name Service** from the next menu.
5. Select **Stop Using Name Service** from the next menu.

A command status screen displays the following message.

Command completed successfully

Domain Name Service is disabled

6. Press **F3 (Esc + 3)** to back up to the Perform System Configuration Changes menu and select **Apply Changes to Configuration Database** to apply the configuration change.

Adding a Name Server: To add a name server:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** from the main menu.
3. Select **Perform System Configuration Changes** from the next menu.
4. Select **Configure Remote Host Name Service** from the next menu.
5. Select **Add a Name Server** from the next menu.
6. Enter the IP address of the name server on the dialog screen. The format for an IP address is *nnn.nnn.nnn.nnn* where *nnn* can be any decimal number from 1 to 255.

A command status screen displays the following message.

Command completed successfully

Node 215.001.230.142 is added as a remote name service host

7. Press **F3 (Esc + 3)** to back up to the Perform System Configuration Changes menu and select **Apply Changes to Configuration Database** to apply the configuration change.

Deleting a Name Server: To delete a name server:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** from the main menu.
3. Select **Perform System Configuration Changes** from the next menu.
4. Select **Configure Remote Host Name Service** from the next menu.
5. Select **Delete a Name Server** from the next menu.
6. On the selector screen, select the IP address of the name server that you want to delete.

A command status screen displays the following message.

Command completed successfully

Node 215.1.230.142 is deleted from the list of name service hosts

7. Press **F3 (Esc + 3)** to back up to the Perform System Configuration Changes menu and select **Apply Changes to Configuration Database** to apply the configuration change.

Configuring Remote Time Service

Remote time service is a mechanism for the IBM 6611 to get its time from another IP node on the network. When enabled, this IBM 6611 gets its time from the first remote time server listed in the list of remote time servers by sending a time service request. If the first remote time server listed is unable to provide time service, the request is sent to the second remote time server in the list. Figure 10-17 displays the Configure Remote Time Service menu.

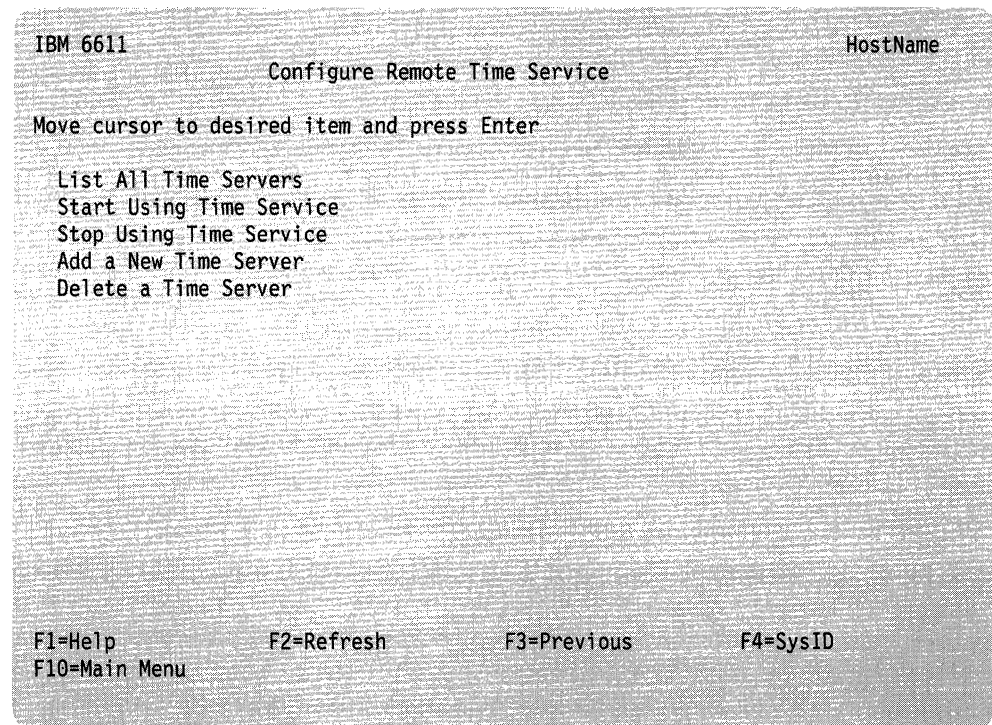


Figure 10-17. Configure Remote Time Service Menu

See the following pages for more information about the individual menu items:

Listing All Time Servers	10-40
Start Using Time Service	10-40
Stop Using Time Service	10-40
Adding a Time Server	10-41
Deleting a Time Server	10-41

You can invoke these tasks using command primitives. See "Time Server Command Primitives" on page 8-87 for information about the command primitives.

Listing All Time Servers: To list all time servers using the System Manager:

1. Select **System Environment and Configuration** on the System Manager main menu.
2. Select **Perform System Configuration Changes** from the next menu.
3. Select **Configure Remote Time Service** from the next menu.
4. Select **List All Time Servers** from the next menu.

A command status screen displays a listing all of timer servers. For example,

IP Address of Remote Time Server:
215.1.230.142

Start Using Time Service: To start using time service:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** on the System Manager main menu.
3. Select **Perform System Configuration Changes** from the next menu.
4. Select **Configure Remote Time Service** from the next menu.
5. Select **Start Using Time Service** from the next menu.

A command status screen displays the following message.

Command completed successfully
Time Service is started.

6. Press **F3 (Esc + 3)** to back up to the Perform System Configuration Changes menu and select **Apply Changes to Configuration Database** to apply the configuration change.

Stop Using Time Service: To stop using time service:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** on the System Manager main menu.
3. Select **Perform System Configuration Changes** from the next menu.
4. Select **Configure Remote Time Service** from the next menu.
5. Select **Perform System Configuration Changes** from the next menu.
6. Select **Stop Using Time Service** from the next menu.

A command status screen displays with the following message:

Command completed successfully
Time Service is stopped.

7. Press **F3 (Esc + 3)** to back up to the Perform System Configuration Changes menu and select **Apply Changes to Configuration Database** to apply the configuration change.

Adding a Time Server: To add a time server using the System Manager:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** on the System Manager main menu.
3. Select **Perform System Configuration Changes** from the next menu.
4. Select **Configure Remote Time Service** from the next menu.
5. Select **Add a Time Server** from the next menu.
6. Type in the IP address of the timer server you want to add on the dialog screen. The format for an IP address is *nnn.nnn.nnn.nnn* where *nnn* can be any decimal number from 1 to 255.

A command status screen displays the following message:

```
Command completed successfully
Node 215.001.243.142 is added as a remote time service host.
```

7. Press **F3 (Esc + 3)** to back up to the Perform System Configuration Changes menu and select **Apply Changes to Configuration Database** to apply the configuration change.

Deleting a Time Server: To delete a timer server using the System Manager:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** on the System Manager main menu.
3. Select **Perform System Configuration Changes** from the next menu.
4. Select **Configure Remote Time Service** from the next menu.
5. Select **Delete a Time Server** from the next menu.
6. On the selector screen, select the IP address of the time server that you want to delete.

A command status screen displays the following message:

```
Command completed successfully
Node 215.1.243.142 is deleted from the list of remote time service hosts.
```

7. Press **F3 (Esc + 3)** to back up to the Perform System Configuration Changes menu and select **Apply Changes to Configuration Database** to apply the configuration change.

Apply Changes to Configuration Database

The System Manager method of configuring the IBM 6611 includes an apply, test, and either commit or reject scenario. The configuration changes are *applied* and *tested* in an actual test environment, and then either *committed* if the changes are approved, or *rejected* if the changes are not approved.

Only a controlling user can update configuration parameters.

Whenever you make a configuration change, the System Manager Configuration Facility updates a local configuration copy which is stored in the home directory of your userid. The System Manager Configuration Facility adds the configuration

changes to the global configuration copy, when you apply the change. The configuration change becomes a part of the running configuration only after you apply it. If you log off your userid before applying the changes, you have not lost them. The local configuration copy retains the unapplied changes, along with all your applied changes. Applied changes that have not been committed, have a saved backup version associated with them.

Warning: Make all System Manager configuration changes from the same controlling userid to minimize the chance of overriding another user's configuration changes.

To apply changes to a configuration database using the System Manager:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** on the System Manager main menu.
3. Select **Perform System Configuration Changes** from the next menu.
4. Select **Apply Changes to Configuration Database** from the next menu.

A command status screen displays the following message:

```
Waiting for acknowledgement from config daemon ... done.  
Command completed successfully
```

Commit Changes to Configuration Database

The System Manager Configuration Facility deletes the local backup copy of the configuration when the configuration is committed. You cannot reject a committed configuration change. If you commit your configuration changes, you will not be able to return to the previous configuration, unless you manually undo each change you make. You have the choice of committing only your applied changes or both your applied and unapplied changes.

To commit changes to a configuration database using the System Manager:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** on the System Manager main menu.
3. Select **Perform System Configuration Changes** from the next menu.
4. Select **Commit Changes to Configuration Database** from the next menu.
5. On the selector screen, select **only applied changes** to commit only the applied changes. Select **applied and unapplied changes** to commit both the applied and unapplied changes.

A command status screen displays the following message:

```
Waiting for acknowledgement from config daemon ... done.  
Command completed successfully
```

Reject Uncommitted Changes to Configuration Database

If you issue a reject, the System Manager Configuration Facility removes the configuration changes you choose to reject. You have the choice of rejecting only your unapplied changes or both your applied and unapplied changes. The unapplied changes are removed from your local copy of the configuration and the applied changes are removed from the local copy and the global copy of the configuration. The Configuration Facility replaces the local copy of the configuration with the local backup copy.

To cancel uncommitted changes to a configuration database using the System Manager:

1. Log in using a controlling userid.
2. Select **System Environment and Configuration** on the System Manager main menu.
3. Select **Perform System Configuration Changes** from the next menu.
4. Select **Reject Uncommitted Changes to Configuration Database** from the next menu.
5. On the selector screen, select **only unapplied changes** to reject only the unapplied changes. Select **applied and unapplied changes** to reject both the applied and unapplied changes.

A command status screen displays the following message:

```
Waiting for acknowledgement from config daemon ... done.  
Command completed successfully
```

Transferring Files

You can transfer files to and from the IBM 6611 using:

- FTP
- Xmodem protocol
- Diskettes (DOS or UNIX).

A file transferred into the IBM 6611 is placed in the *transfer directory*. A file, that needs to be transferred out of the IBM 6611, must be in either the *transfer directory* or the *static directory*.

The System Manager has two menu items to manage files:

- Work with Files in Transfer Directory
- View a File in Static Directory.

See "Working with Files in the Transfer Directory" on page 10-19 and "Viewing a File in the Static Directory" on page 10-21 for information about using these System Manager tasks.

File Names for Output in Transfer Directory

A file transferred into the IBM 6611 is placed in the *transfer directory*. A file, that needs to be transferred out of the IBM 6611, must be in either the *transfer directory* or the *static directory*.

You can view, rename, delete and transfer the files in the transfer directory. Most of the files are in ASCII format. A few of the files are in binary format. None of the files are EBCDIC. You can determine which files are binary because the files appear as a memory dump when they are browsed. The static directory holds special files placed there by system components that allow the files to be viewed or transferred out of the IBM 6611, but do not allow them to be deleted or renamed.

There are various areas in the System Manager and in the fast-path environment where data is generated. Most of the files in the transfer directory are placed there because you selected the **transfer_directory** as the destination when executing a System Manager function. If the output from a fast-path command primitive is long, it is sent directly to the transfer directory. In each of the cases where the output is

directed to the transfer directory, the file name is set by the IBM 6611. You can find these file names in the tables starting with Table 10-2 on page 10-46 through Table 10-7 on page 10-49. You can find other files not created or used by System Manager processes in Table 10-8 on page 10-50.

You should delete unneeded files that you create from the transfer directory in a timely manner to prevent the transfer directory from becoming full.

A few files in the transfer directory are trace logs. The size of these files can increase. Most of these are not started by System Manager commands. Do not erase these files, unless you are instructed to do so by IBM service personnel.

These trace log files all have a limit. When these files reach their size limit, a pruning process copies them into a file with the same name and an extension of *mondisk.2* appended to the end. The pruning process zeros the original file and the trace continues to write into the file. The trace file with the *mondisk.2* extension contains the earliest trace data. You can find the file names for these pruned files in Table 10-9 on page 10-50.

For example, the limit of the system monitor trace log is 500 Kb. The output of the trace is written into *pd_sysmon.trc*. When *pd_sysmon.trc* reaches 500 Kb, the pruning process copies the trace files into *pd_sysmon.trc.mondisk.2* overlaying the existing data in that file. The *pd_sysmon.trc* file is zeroed and tracing continues.

The pruning process monitors the file system of the transfer directory. When it becomes 97% full, it removes certain files from the transfer directory that have been targeted for removal. These targeted files include all generated reports, statistics, vital product data, and dumps and most problem determination output. Wildcards (*) are used to locate the files to remove. You can find the file names for these removed files in Table 10-10 on page 10-50.

If this removal does not reduce the file system of the transfer directory to below 97%, the pruning process removes all the files in the transfer directory that are over 2 days old, except for the special trace files, that it continues to prune. If this additional removal does not reduce the file system of the transfer directory to below 97%, the pruning process removes all the files in the transfer directory regardless of how long they have existed, except for the special trace files that it continues to prune.

The pruning process does not remove any software installation packages that are in the transfer directory. These should be removed by the Software Installation and Maintenance Facility after the software is installed.

Most of the data generated is for problem solving and the contents of the files are analyzed only by IBM service personnel. This book does not explain the content of most of these files, except for the error report. See "Contents of an Error Record" on page 11-5 for details about reading an error report.

In each of the locations where the data can be sent to the screen or to the transfer directory, a selector screen displayed in Figure 10-18 on page 10-45 appears:

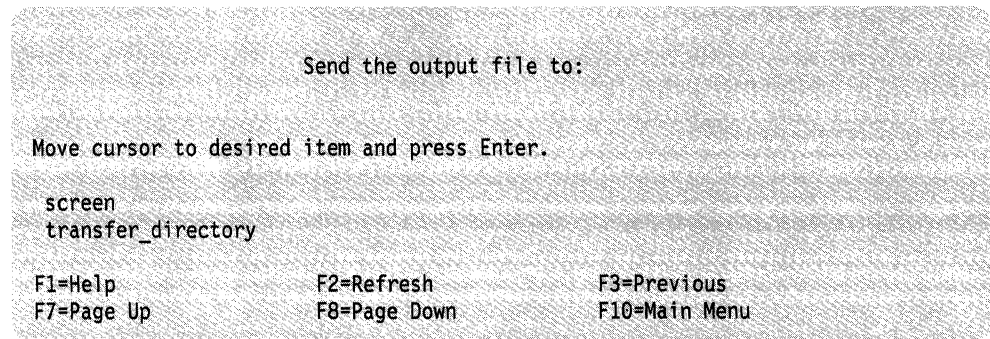


Figure 10-18. Pop-Up Screen Used to Direct Output

Select the transfer directory, if you want the output to be stored in a file to view later or to transfer out of the IBM 6611.

Table 10-2. Output File Names Generated from Performance and Statistics Menu Items

Performance and Statistics menu item	Items on next menu	File names in transfer directory
View System Activity Report		ps_sar.report
View Process Information and Status	View Process Information	ps_proc.info
	View Process Status	ps_proc.stat
	View Process Table Information	ps_proctab.info
View Adapter Interface Statistics (see notes about <i>intf</i> values below)	Connection Statistics	ps_intf_proto_con.stat
	Protocol Statistics	ps_intf_proto_proto.stat
	Filter Information	ps_intf_proto_filter.info
	Packet Traffic Statistics	ps_intf_packet.stat
	Bridge Statistics	ps_intf_adp_bridge.stat
	LAN Bridge Statistics	ps_intf_adp_lan_bridge.stat
View System Network Statistics	Connection Statistics	ps_net_con.stat
	TCP/IP Protocol Statistics	ps_net_proto.stat
	Packet Traffic Statistics	ps_intf_net_packet.stat
	Memory Management Statistics	ps_net_mem.stat
	TCP/IP Route Statistics	ps_net_route.stat
	System Socket Information	ps_net_socket.stat
	Active Internet Connection Information	ps_net_inet.info
	Source Route Bridge Spanning Tree Statistics	ps_intf_srb_sptree.stat
	Source Route Bridge Spanning Tree Frame Relay Statistics	ps_intf_srb_sptree_fr.stat
	Transparent Bridge Spanning Tree Statistics	ps_intf_tb_sptree.stat
	Transparent Bridge Spanning Tree Frame Relay Statistics	ps_intf_tb_sptree_fr.stat
	LAN Bridge Statistics	ps_intf_lan_bridge.stat
	LAN Bridge Internal Protocol Frame Statistics	ps_intf_lan_bridge_fr.stat
View Virtual Memory Statistics		ps_virt_mem.stat
View Input/Output Statistics		ps_io.stat

Notes:

1. *intf* values lo0 and lo1 are for loopbacks.
2. *intf* values to0, to1, to2, to3, to4, to5, to6, to7, to8, to9, to10, to11, to12, and to13 are for EIA 422/449 Serial Adapter and V.35/V.36 Serial Adapter interfaces.
3. *intf* values te0, te1, te2, te3, te4, te5 , and te6 are for Ethernet Adapter interfaces.
4. *intf* values tk0, tk1, tk2, tk3, tk4, tk5 , and tk6 for Token-Ring Network 16/4 Adapter interfaces.
5. *intf* values xt0, xt1, xt2, xt3, xt4, xt5 , and xt6 are for X.25 Adapter interfaces.
6. *proto* values are DECnet, IP, IPX and XNS.

See Table 10-1 on page 10-8 for numbering information.

Table 10-3 (Page 1 of 2). Output File Names Generated from Problem Determination Facilities Menu Items

Problem Determination Facilities menu Item	Items on next menu	File names in transfer directory
View an Error Report		pd_error.report
View an Error Report for a Single Sequence Number (see note 1 on page 10-48)		pd_error.nnnn.report
Use System and User Process Dump Facilities	Copy System Dump to Diskette or Transfer Directory	pd_system.dump
	View a Formatted System Dump	pd_system.fdump
	View User Process Memory Dump (see note 2 on page 10-48)	pd_dump.process.nnnn
	Start APPN User Process Memory Dump	pd_dump.APPN.dn
Use System Trace Facility	Start IP Routing Protocols Dump	pd_route_proto_dump
	View System Trace Report	pd_trace.report
	Use IP Routing Protocols Trace then Start IP Routing Protocols Trace	pd_route_proto.trc
	View SNMP Trace (see notes 3 and 4 on page 10-48)	pd_snmpd.log pd_snmpd.log.n pd_cfgd.logn pd_dlsd.logn pd_pppd.logn pd_r66d.logn pd_rs960d.logn pd_t1d.logn pd_trapd.logn
Use Special User Process Traces	View System Monitor Trace	pd_sysmon.trc pd_sysmon.trc.mondisk.2
	View X.25 Trace	pd_x25d.out pd_x25d.out.mondisk.2
	View APPN Trace Report	pd_trace.report
	View AppleTalk Protocol Trace	pd_appletalk.trc
Use Adapter Debug Facility (see notes 5, 6, and 7 on page 10-48)	Read Adapter Memory	pd_adapter.read
	Start Adapter Line Trace	pd_adapter.linetrace
	Dump Adapter Memory	pd_adapter.regs pd_adapter.dram pd_adapter.sram pd_adapter.prom

Table 10-3 (Page 2 of 2). Output File Names Generated from Problem Determination Facilities Menu Items

Problem Determination Facilities menu item	Items on next menu	File names in transfer directory
Use Source Route Bridging Debug Facility (see notes about <i>intf</i> values on page 10-46)	View Bridge Trace Files	pd_sptmain pd_sptmain.mondisk.2 pd_bnbmast pd_bnbmast.mondisk.2 pd_bnbrifh pd_bnbrifh.mondisk.2 pd_bnbxipf pd_bnbxipf.mondisk.2 pd_bnbmanp pd_bnbmanp.mondisk.2 pd_tbstmain pd_tbstmain.conf pd_tbstcfdg pd_tbstcfdg.conf
	View Bridging Frame Trace Output	pd_bframe_b_ <i>intf</i> pd_bframe_r_ <i>intf</i> pd_bframe_t_ <i>intf</i>
	View Bridge Configuration Information	pd_config. <i>intf</i>
	View Bridge SAP Filter Information	pd_bsap. <i>intf</i> .
Copy Error Log or Trace Log to Transfer Directory		pd_error.log pd_trace.log

Notes:

1. *nnnn* is the sequence number
2. *process* is the process name and *nnnn* is a sequence number from the error log
3. *log.n* = log.0, log.1, log.2, or log.3
4. *logn* = log, log1, log2, or log3
5. *adapter* values entya0, entya1, entya2, entya3, entya4, entya5, and entya6 are for Ethernet Adapters
6. *adapter* values trtya0, trtya1, trtya2, trtya3, trtya4, trtya5, and trtya6 are for Token-Ring Network 16/4 Adapters
7. *adapter* values t1tya0, t1tya1, t1tya2, t1tya3, t1tya4, t1tya5, t1tya6, t1tya7, t1tya8, t1tya9, t1tya10, t1tya11, t1tya12, and t1tya13 are for EIA 422/449 Serial Adapter.

See Table 11-1 on page 11-37 for numbering information.

Table 10-4. Output File Names Generated from Resource Control and Management Menu Items

Resource Control and Management menu item	Items on next menu	File names in transfer directory
View System Route Table		system.routes
View Adapter Route Tables (see notes about <i>intf</i> values below)		<i>intf</i> .routes. <i>proto</i>
View Network Management Subsystem Information		pd_snmpd.info

Notes:

1. *intf* values to0, to1, to2, to3, to4, to5, to6, to7, to8, to9, to10, to11, to12, and to13 are for EIA 422/449 Serial Adapters
2. *intf* values te0, te1, te2, te3, te4, te5, and te6 are for Ethernet Adapters
3. *intf* values tk0, tk1, tk2, tk3, tk4, tk5, and tk6 are for Token-Ring Network 16/4 Adapters.
4. *proto* values are DECnet, IP, IPX and XNS.

See Table 10-1 on page 10-8 for numbering information.

Table 10-5. Output File Names Generated from Software Installation and Maintenance Menu Items

Software Installation and Maintenance menu item	Items on next menu	File names in transfer directory
View Software Vital Product Data (see note about <i>comp.name</i> values below)	List All Installed Software	vpd_softall.list
	List All Updates to a Software Component	vpd_softchg.all vpd_softchg.comp.name
	List Files Included in a Software Component	vpd_softfile.comp.name
	List Prerequisites of a Software Component	vpd_softpre.all vpd_softpre.comp.name
	List Dependents of a Software Component	vpd_softdep.all vpd_softdep.comp.name
	View ID of a Software Component	vpd_softid.all vpd_softid.comp.name
	View History of a Software Component	vpd_softhis.all vpd_softhis.comp.name

Note: *comp.name* is either *mpnp.obj* or *mpnp.data*.

Table 10-6. Output File Names Generated from Hardware Vital Product Data Menu Items

Hardware Vital Product Data menu item	Items on next menu	File names in transfer directory
List All Supported Devices		vpd_supdev.list
List All Defined Devices		vpd_defdev.list
List All Installed Devices		vpd_instldev.list
View Characteristics of a Defined Device (see note about <i>device</i> values below)		vpd_device.char
View Hardware Vital Product Data		vpd_hardware.vpd

Note: *device* is any device in the "Defined devices" selector window (such as *aio0*, *bus0*, *fd0*).

Table 10-7. Output File Names Generated from Configuration Files and Reports Menu Items

Configuration Files and Reports menu item	Items on next menu	File names in transfer directory
View Configuration Report		config.report.brief config.report.detailed
View Configuration Error Messages		config.errmsgs
View Configuration Script		config.script
Import Binary Configuration File		config
Export Binary Configuration File		config

Table 10-8. Output File Names not Generated from System Manager

File name in transfer directory

pd_pppsysmond.log
pd_lcpd.log
pd_dnarouted.log
console
mail
sysman.trace

Table 10-9. Output File Names for Pruned Files

File name in transfer directory	Upper limit
pd_sysmon.trc	500K
pd_x25d.out	10K
pd_sptmain	100K
pd_bnbmast	100K
pd_bnbrifh	100K
pd_bnpxipt	100K
pd_bnpmanp	100K
pd_pppsysmond.log	100K
pd_lcpd.log	100K
pd_dnarouted.log	160K
console	10K
mail	10K
pd_appletalk.trc	100K
pd_tbstmain	100K
pd_tbstmain.conf	50K
pd_tbstcfgd	100K
pd_tbstcfgd.conf	100K

Table 10-10. Output File Names for Removed Files

File name groupings
log
*trace
config.rep*
vpd_*
ps_*
pd_config*
pd_bsap*
config.scr*
.route
dump
*.out
pd_adapter*
*.report
*.errmsgs
dump
*.mondisk.2

Exporting Specific Data

There are several places in the System Manager where specific menu items exist for transferring generated data out of the IBM 6611. In each of these cases, the files that you are allowed to transfer out are specific to the menu item. Use the list below to locate the particular menu item for the file you want to transfer.

- Export Performance Data
 - Select **Performance and Statistics** on the main menu.

- Export Software Vital Product Data
 - Select **Software Installation and Maintenance** on the main menu.
 - Select **View Software Vital Product Data** on next menu.
- Export Hardware Vital Product Data
 - Select **Hardware Vital Product Data** on the main menu.
- Export Problem Determination Output
 - Select **Problem Determination Facilities** on the main menu.
- Export Route Information
 - Select **Resource Control and Management** on the main menu.
- Export Configuration Information
 - Select **Configuration Files and Reports** on the main menu.
- Export Binary Configuration File
 - Select **Configuration Files and Reports** on the main menu.

In each of these cases, a selector screen appears requesting you to select the transfer method. The transfer methods available on most of these selector screens are:

- FTP
- Modem
- DOS diskette
- UNIX diskette.

With each of these file transfer methods, a selector screen appears requesting the name of the file to be transferred. The list is specific to the menu item. See “Using the File Transfer Protocol” on page 10-52 to get further instructions about sending a file using FTP. See “Using the Xmodem Protocol” on page 10-55 to get further instructions on sending a file using Xmodem.

Importing Specific Data

There are also specific menu items for transferring specific files to the IBM 6611. The only type of files to import to the IBM 6611 are software updates and the binary configuration file. The transfer methods used to import files from a workstation are as follows:

- FTP
- Modem
- Diskette.

The IBM 6611 receives software updates on a diskette in install format. The IBM 6611 receives the binary configuration files on diskettes in DOS format. Use the list below to locate the particular menu item for the file you want to import.

- Import Binary Configuration File
 - Select **Configuration Files and Reports** on the main menu.
- Import Software to Transfer Directory
 - Select **Software Installation and Maintenance** on the main menu.

Exporting Files to a Remote Node

To transfer any file from the transfer directory or the static directory to a remote node:

1. Select **Remote Accesses to Other Nodes** on the main menu.
2. Select **Send Files to Another Node** from the next menu.
3. Select the transfer method, either **FTP** or **modem** from the selector screen.
4. Select the directory from which to send a file, either the **transfer directory** or the **static directory** from the next selector screen.

Importing Files from a Remote Node

To transfer any file to the transfer directory from a remote node:

1. Select **Remote Accesses to Other Nodes** on the main menu.
2. Select **Receive Files from Another Node** from the next menu.
3. Select the transfer method, either **FTP** or **modem** from the selector screen.

It may be necessary also to transfer files in and out of the IBM 6611 using diskettes. See "Performing Diskette Operations" on page 10-22 to get further instructions about sending and receiving files from diskettes and performing other diskette operations.

Using the File Transfer Protocol

FTP allows file transfer between an IBM 6611 and another IP node, for example another IBM 6611. The IBM 6611 can issue and receive FTP requests. To transfer files using FTP, specify some or all of the following information:

- Host name or IP address of the IP node that is sending or receiving the file
- Userid and password of a user at the remote IP node
- Filename to be transferred
- Type of transfer (get or put)
- Type of file (binary or ASCII).

You can use only a limited number of **ftp** subcommands, when you issue **ftp** from a remote IP host to the IBM 6611. The commands are as follows:

get	Sends a file from the IBM 6611 to the remote IP host.
mget	Sends multiple files from the IBM 6611 to the remote IP host.
put	Copies a file from the remote IP host to the IBM 6611
mput	Copies multiple files from the remote IP host to the IBM 6611
cd /static	Changes the current directory to the static directory. The current directory must be the static directory in order to transfer files from the static directory.
cd /transfer	Changes the current directory to the transfer directory. The current directory must be the transfer directory in order to transfer files to or from the transfer directory.
ls	Lists the files in the current directory, either the transfer directory or the static directory.

If a file is to be transferred into a remote IP node, that is not an IBM 6611, the file is added (put) in the home directory for the specified userid. If a file is to be retrieved

from the remote IP node, it is retrieved (get) from the home directory of the remote IP node. If a file is to be transferred to an IBM 6611, it is placed in the transfer directory. If a file is to be transferred from an IBM 6611, it is taken from either the transfer directory or the static directory.

There are two versions of FTP used by the IBM 6611:

Single line version All options specified first, (except the password prompt)

Interactive version FTP initiated with only the host name; all other information is prompted.

In the single line version, the System Manager dialog screen lists all the required parameters. You can specify them in the entry field or by using F6 (Esc + 6). Press **Enter** after specifying all the required fields. You are prompted for the password. Each of the System Manager menu items uses this type of FTP, except those on the Remote Accesses to Other Nodes menu. Only the **get** and **put** FTP subcommands are correct with the single line version.

The **Send Files to Another Node** and **Receive Files from Another Node** menu items on the Remote Accesses to Other Nodes menu use the interactive version of FTP. The **ftp** command from the fast-path environment also uses this version.

With the interactive version, a typical scenario is as follows:

- Select **Remote Accesses to Other Nodes** from the main menu.
- Select **Send Files to Another Node** from the next menu.
- Select **FTP** from the selector screen.
- Select **transfer_directory** from the next selector screen.
- Enter the **Host name** on the dialog screen.

Output displayed:

```
Trying to connect to hostname
Once successfully connected, you may send a file
from the transfer directory by typing
    put <file_name>
at the ftp prompt
```

```
To quit an FTP session and return to System Manager
Type 'quit' at the ftp prompt
```

```
Press Any Key to Continue ..
```

Type in: Press any key

Output displayed:

```
Connected to hostname.
220 hostname ftp server (Version 4.1 Date) ready.
Name (hostname: local_userid):
```

Type in:

```
Name (hostname: local_userid): remote_userid
```

Output displayed:

```
331 Password required for remote_userid.  
Password:
```

Type in: (Enter the password. It will not be displayed.)

Output displayed:

```
230 User remote_userid logged in.  
ftp>
```

Type in:

```
ftp> put file_name
```

Output displayed:

```
200 PORT command successful.  
150 Opening ASCII mode data connection for file_name.  
226 Transfer complete.  
13029 bytes sent in 0.07388 seconds (172.2 Kbytes/s)  
>ftp
```

Type in:

```
ftp> quit
```

Output displayed:

```
221 Goodbye.
```

The numbers associated with the FTP messages are standard message numbers for this protocol. They have no significance other than to identify the message. Figure 10-19 shows the Remote Accesses to Other Nodes menu.

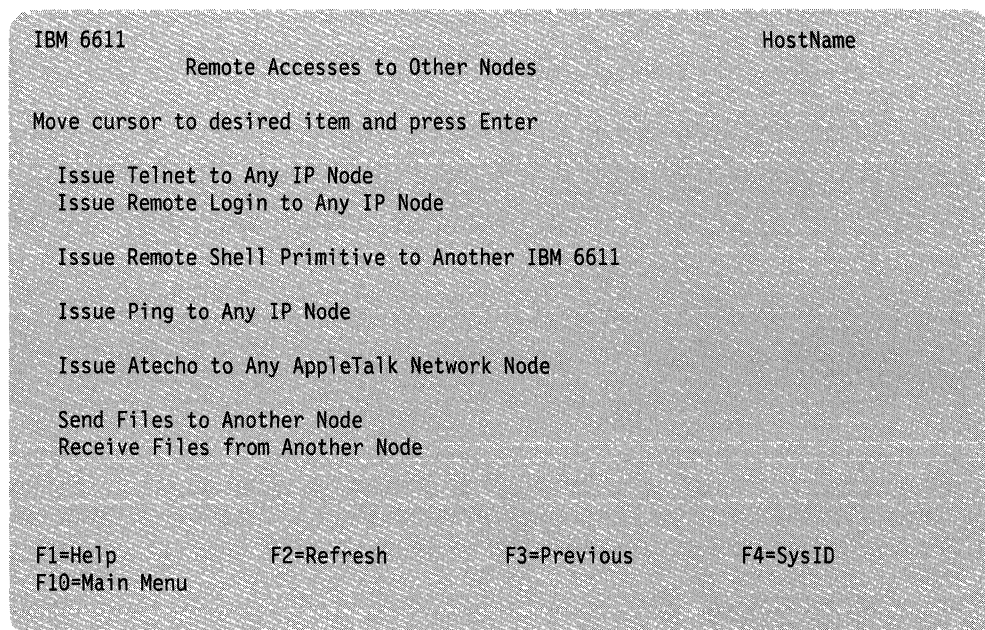


Figure 10-19. Remote Accesses to Other Nodes

Using the Xmodem Protocol

The Xmodem protocol is an 8-bit transfer protocol that can detect data transmission errors and then retransmit the data. The station that sends the data waits until the remote station sends a signal that it is ready to receive data. When the remote station gets the data, it returns an acknowledgment to the sender. Sending and receiving files with the Xmodem command are complementary operations. One system must be set to send while the other is set to receive. To interrupt the Xmodem file transfer, press **Ctrl + X**.

To transfer files between an IBM 6611 and a local workstation via Xmodem:

1. Establish the connection between the local workstation and the IBM 6611 with the attached modem. Refer to the documentation about the Xmodem protocol in the manual supplied with the communications package for the exact syntax.
2. A login prompt appears. You are requested to type in a userid and password.
3. If the file transfer is between an IBM 6611 that is not equipped with the modem and the workstation from which the telephone connection was made, then an RLOGIN network connection is needed from the IBM 6611 or other IP node equipped with the modem and the IBM 6611 from which or to which the file is to be transferred. See "Using Remote Login" on page 9-10 for details about establishing a remote login connection.
4. When the login has completed to the IBM 6611 needing a file transfer, you are in the System Manager. There are several menu items pertaining to transferring files via modem access. Use the System Manager menus to find the menu item relating to the file transfer needed.
5. Select the file name you want to transfer. The IBM 6611 issues the message:

```
Sending (Receiving) file file_name via Xmodem  
You can return to local machine and begin file transmission.
```
6. Return to the local machine (the one that initiated the telephone call) using the key sequence defined by the communication program.
7. Receive or send the file, and wait until the file transfer completes.
8. When the file has been transferred, return to the IBM 6611 by reconnecting using the communication program.

Transferring Files between a RISC System/6000 and IBM 6611

To establish a remote login session between a RISC System/6000 workstation and the IBM 6611 using a modem, use the Asynchronous Terminal Emulation (ATE) program located on the RISC System/6000 workstation. The ATE program allows you to establish a connection between the RISC System/6000 workstation and the IBM 6611. The workstation acts as a terminal connected to the IBM 6611. Using ATE, you can run commands on the IBM 6611 and send and receive files using Xmodem.

The ATE program is menu driven and uses subcommands. The RISC System/6000 ATE program has a dialing directory feature that is a list of up to 20 frequently dialed phone numbers. The dialing directory contains the telephone number and other connection information such as baud rate, parity, and the name of the host at the other end of the connection. The **directory** subcommand allows you to display the telephone numbers and select the one you need to connect to the system you are calling, instead of entering the phone number with the connect subcommand. The **send** subcommand is used to send files from the RISC System/6000 workstation to the IBM 6611. The **receive** subcommand is used to receive files from the IBM

6611 to the RISC System/6000 workstation. The subcommands are entered from the appropriate menu by typing in the first letter of the subcommand followed by the command parameters.

Use the following scenarios to connect to the IBM 6611, and send or receive files from the RISC System/6000 workstation. To send a file from IBM 6611 to RISC System/6000 workstation:

1. To start the ATE program, type **ate** on the command line of the RISC System/6000 workstation.
2. The ATE Unconnected Main Menu is displayed. Using the ATE menus, set the following values:

Terminal type	VT100
Line speed	2400 bps
Transfer Protocol	Xmodem
3. From this menu, type either the **connect** or **directory** subcommand to connect to the IBM 6611.
 - To use the **connect** subcommand, type **c telephone_number**.
 - To use the **directory** subcommand, type **d**.A list of remote station names and phone numbers appears. Select the one corresponding to the IBM 6611 which needs a file transfer.
4. The remote connection is made. Enter the login information when prompted.
 - Userid
 - Password
 - Terminal type.
5. You are automatically placed in the System Manager. Find the menu item you want to use to transfer the file to the RISC System/6000 workstation or go to the fast-path environment and enter the following command primitive to send a file from either the transfer or static directory.

modem_send directory_name file_name
6. Press **Ctrl + V** (main menu key) at the RISC System/6000 workstation to return to ATE. The ATE Connected Main Menu is displayed.
7. Type the receive subcommand as follows: **r file_name**. The **receive** subcommand instructs the workstation to receive the file from the remote IBM 6611.
8. After transferring the file, the ATE program displays the Connected Main Menu.

To receive a file at the IBM 6611 from the RISC System/6000 workstation:

1. To start the ATE program, type **ate** on the command line of the RISC System/6000 workstation.
2. From this menu, issue either the **connect** or **directory** subcommand to connect to the IBM 6611.
 - To use the **connect** subcommand, type **c telephone_number**.
 - To use the **directory** subcommand, type **d**.

A list of remote station names and phone numbers appears. Select the one corresponding to the IBM 6611 needing a file transfer.

3. The remote connection is made. Enter the login information when prompted.
 - Userid
 - Password
 - Terminal type.
4. You are automatically placed in the System Manager. Find the menu item you want to use to transfer the file from the RISC System/6000 workstation or go to the fast-path environment and enter the following command primitive to receive a file from the current directory of the RISC System/6000 into the transfer directory of the IBM 6611.
modem_rcv file_name.
5. Press **Ctrl + V** (main menu key) at the RISC System/6000 workstation to return to ATE on the workstation. The ATE Connected Main Menu is displayed.
6. Type the **send** subcommand as follows: **s file_name**. The **send** subcommand instructs the workstation to send the file to the remote IBM 6611.
7. After transferring the file, the ATE program displays the Connected Main Menu.

Transferring Files to Diskette

In many cases, it is not possible to transfer files remotely, specifically large files such as a system dump or a trace report. In order to get the information to IBM service personnel, it is necessary to put the data on a diskette.

The System Manager supports transferring the data on a diskette in either DOS or UNIX format. However, a file transferred to a DOS diskette must be small enough to fit on a single diskette. There is a special command for transferring the system dump to diskettes, Copy System Dump to Diskette or Transfer Directory. See "Performing Diskette Operations" on page 10-22 for more information on transferring other files to diskette.

Selling the IBM 6611 to a Third Party

When the IBM 6611 is sold to a third party, the original owner must lock the Multiprotocol Network Program using either the Configuration Program or a fast-path command primitive. The software is locked by the original owner and unlocked by the customer to whom it is sold.

To lock the Multiprotocol Network Program using the Configuration Program:

1. Select **System Management** from the main window of the Configuration Program.
2. Select **Lock** as the lock value from the next window. The default value is unlock.
3. Create a startup diskette with this parameter.
4. Place the startup configuration diskette in the diskette drive of the IBM 6611. Press **Reset**. After the system restarts, the IBM 6611 locks the Multiprotocol Network Program.

To lock the Multiprotocol Network Program using a fast-path environment command primitive:

1. Press **F3** on the main menu of the System Manager to enter the fast-path command environment.
2. Type **sw_lock** on the command line.

To unlock the Multiprotocol Network Program using the Configuration Program:

1. Select **System Management** from the main window of the Configuration Program.
2. Select **Unlock** as the lock value from the next window. This is the default value.
3. Create a startup diskette with this parameter.
4. Place the startup configuration diskette in the diskette drive of the IBM 6611. Press the **Reset** button. The Multiprotocol Network Program will unlock when the system restarts.

You cannot unlock the Multiprotocol Network Program from the fast-path environment.

Chapter 11. Problem Determination

About This Chapter	11-3
Problem Determination Facilities Provided by the System Manager	11-3
Selecting a Problem Determination Facility	11-3
Using the IBM 6611 Problem Determination Facilities	11-3
Error Log Facility Overview	11-4
Contents of an Error Record	11-5
Generating an Error Report	11-6
View an Error Report	11-6
View an Error Report for a Single Sequence Number	11-8
Clean the Error Log	11-10
Use System and User Process Dump Facilities	11-11
Start System Dump	11-12
View Previous System Dump Information	11-13
Copy System Dump to Diskette or Transfer Directory	11-14
View a Formatted System Dump	11-14
Extract Error Log Records From System Dump	11-15
Extract Trace Log Records From System Dump	11-15
Start APPN User Process Memory Dump	11-16
Start User Process Memory Dump	11-16
View User Process Memory Dump	11-17
Start IP Routing Protocols Dump	11-19
View IP Routing Protocols Dump	11-19
Use System Trace Facility	11-21
Start System Trace	11-21
Stop System Trace	11-22
View System Trace Report	11-22
Use Special User Process Traces	11-24
Use IP Routing Protocols Trace	11-25
Start IP Routing Protocols Trace	11-25
Stop IP Routing Protocols Trace	11-26
View IP Routing Protocols Trace	11-26
Start and Stop SNMP Trace	11-28
View SNMP Trace	11-28
View System Monitor Trace	11-29
View X.25 Trace	11-30
Use AppleTalk Trace	11-31
Start AppleTalk Protocol Trace	11-31
Stop AppleTalk Protocol Trace	11-32
View AppleTalk Protocol Trace	11-32
Use APPN Trace	11-34
Start APPN Trace	11-34
Stop APPN Trace	11-35
View APPN Trace Report	11-35
Use Adapter Debug Facility	11-37
Read Adapter Memory	11-38
View Adapter Registers	11-39
Start Adapter Line Trace	11-39
Dump Adapter Memory	11-41
View Adapter Debug Data in Transfer Directory	11-41
Use Source Route Bridging Debug Facility	11-42
View Bridge Trace Files	11-44
Start Bridging Frame Trace	11-44

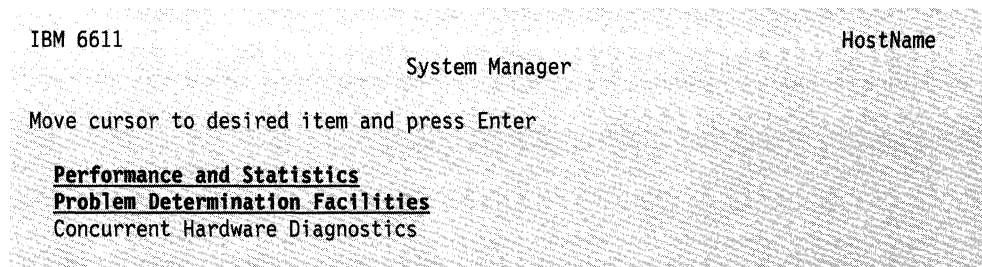
Stop Bridging Frame Trace	11-45
View Bridging Frame Trace Output	11-45
View Bridge Configuration Information	11-46
View Bridge SAP Filter Information	11-47
Use DECnet Debug Facility	11-48
View Routing Data Structures	11-48
Set DECnet Trace Output	11-50
View DECnet Trace Output	11-52
Copy Error Log or Trace Log to Transfer Directory	11-53
Export Problem Determination Output	11-53
Using the IBM 6611 Performance and Statistics Facilities	11-54
View Protocol and Interface Packet Traffic Information	11-55
View Network Management Information	11-57
View System Activity Report	11-59
View Process Information and Status	11-61
List Processes	11-61
List Process Commands	11-62
View Process Information	11-63
View Process Status	11-65
View Process Table Information	11-67
View Adapter Interface Statistics	11-69
Connection Statistics	11-70
Protocol Statistics	11-71
Packet Traffic Statistics	11-72
Filter Information	11-73
Bridge Statistics	11-74
LAN Bridge Statistics	11-75
View System Network Statistics	11-75
Connection Statistics	11-77
TCP/IP Protocol Statistics	11-77
Packet Traffic Statistics	11-79
Memory Management Statistics	11-80
TCP/IP Route Statistics	11-80
System Socket Information	11-81
Active Internet Connection Information	11-81
Spanning Tree Statistics	11-82
Source Route Bridge Spanning Tree Statistics	11-82
Source Route Bridge Spanning Tree Frame Relay Statistics	11-82
Transparent Bridge Spanning Tree Statistics	11-83
Transparent Bridge Spanning Tree Frame Relay Statistics	11-84
LAN Bridge Statistics	11-85
LAN Bridge Internal Protocol Frame Statistics	11-86
View Virtual Memory Statistics	11-87
View Input/Output Statistics	11-88
Export Performance Data	11-89

About This Chapter

This chapter provides information about using the problem determination facilities provided by the System Manager. See Chapter 9 for information about how to access the System Manager.

Problem Determination Facilities Provided by the System Manager

Performance and Statistics and Problem Determination Facilities are selectable from the System Manager main menu as shown below:



Information about using these items on the Performance and Statistics and Problem Determination Facilities menus is included in this chapter. To run diagnostics, see “Running Concurrent Hardware Diagnostics” on page 13-2.

Selecting a Problem Determination Facility

Here are some suggestions on where to start problem determination for various categories of symptoms:

Symptom category	Start here
Code on IBM 6611 3-digit display	See “Reading the Three-Digit Display” on page 10-6 and see Appendix B.
Routing performance complaints	See “View Adapter Interface Statistics” on page 11-69.
User performance complaints	See “View System Activity Report” on page 11-59 and “View System Network Statistics” on page 11-75.
Excessive errors	See “View an Error Report” on page 11-6.
Traps at the network manager or alerts at NetView	Refer to the <i>IBM 6611 Network Processor Network Management Reference</i> .
IBM 6611 stops working	See “Use System and User Process Dump Facilities” on page 11-11.

Using the IBM 6611 Problem Determination Facilities

The following sections describe the various tasks associated with gathering problem determination data that is provided to service the IBM 6611. There are three ways to use these facilities:

- Select items from the System Manager menus
- Issue commands in the fast-path environment
- Issue commands remotely using the **rsh** or **rexec** command.

Figure 11-1 shows the menu screen for Problem Determination Facilities.

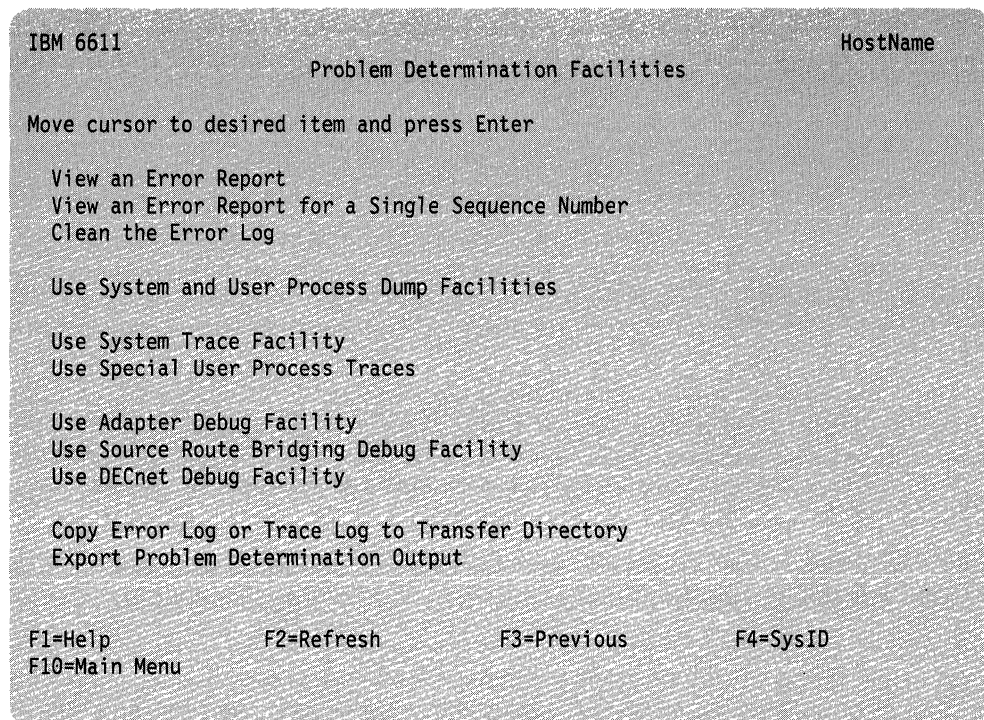


Figure 11-1. Problem Determination Facilities Menu

See these pages for more information about the individual menu items:

View an Error Report	11-6
View an Error Report for a Single Sequence Number	11-8
Clean the Error Log	11-10
Use System and User Process Dump Facilities	11-11
Use System Trace Facility	11-21
Use Special User Process Traces	11-24
Use Adapter Debug Facility	11-37
Use Source Route Bridging Debug Facility	11-42
Use DECnet Debug Facility	11-48
Copy Error Log or Trace Log to Transfer Directory	11-53
Export Problem Determination Output	11-53

Error Log Facility Overview

The Multiprotocol Network Program uses an error log to record activities that occur on the IBM 6611 and the adapters. The IBM 6611 uses the IBM 6611 Error Logging Facility and the IBM 6611 SNMP Trap Facility to communicate error information to you and to IBM service personnel.

Most of the activities recorded in the error log are error conditions. A subset of the errors recorded are classified as "alerts." The alerts are events that require a user response; for example:

Error:	Adapter disabled
Probable Cause:	Hardware failure
User Response:	Call service personnel.

These alerts errors are converted to SNMP traps and transmitted to the network management station, if one exists. The trap data presented at the SNMP network management station tells you the action to perform. In some cases, you receive error notification on the 3-digit display of the IBM 6611.

If the IBM AIX NetView/6000 is used as the SNMP network manager, all traps can be converted to alerts and forwarded to NetView, if desired. Refer to the *IBM 6611 Network Processor Network Management Reference* for more information about using an SNMP network manager and trap information.

Warning: The error log has a capacity of 1 MB and wraps when it is filled. Generally, the entries in the error log should never be deleted. However, entries for specific hardware failures should be deleted after any hardware replacement. Otherwise, any errors in the log from the failed hardware will continue to appear in error reports.

Contents of an Error Record

An error record contains the following information:

- Error label and error ID
- Date and time
- Sequence number
- Machine ID and node ID
- Error class (hardware [H], software[S], or operator[O])
- Resource Name
- Resource class (hardware only)
- Resource type (hardware only)
- Location (hardware only)
- Vital product data (hardware only)
- Error type:

Permanent (PERM)	For conditions when the recovery is unsuccessful.
Performance (PERF)	For conditions that degrade performance of a component (hardware and software) below an acceptable level.
Impending (PEND)	For conditions that signify the loss of a component is threatened.
Temporary (TEMP)	For conditions when the recovery is successful. This error type is also used for non-error events.
Unknown (UNKN)	For conditions when the severity cannot be determined.
- Error descriptions contain messages indicating what caused the event and what action can be taken, if any. There are four types of cause or action messages:
 - Probable cause messages
 - Failure-related error cause or action messages
 - Installation-related cause or action messages
 - User-related cause or action messages.

For each cause or action message, up to four message texts can be displayed. Of the four types of causes, the probable cause message and at least one of the remaining three types of cause messages is provided.

- Detailed data

For software this includes a symptom code with the file name and location where the error was detected.

Generating an Error Report

The error log has up to 1 MB available and wraps when it is filled. The error log facility creates a formatted error report. The error report contains information that is useful to you and to service personnel. The report is sent either to the screen or to a file in the transfer directory. The report can include the whole error log or can be limited by selecting specific values for the following parameters:

- Time intervals
- Resource names
- Resource classes
- Error classes
- Error types
- Error IDs.

The error report can be generated in one of two formats: detailed or summary. The detailed report contains all the data in the error record in readable form. The summary report contains:

- The event ID value
- The timestamp
- The severity
- The event class
- The resource name
- The event description message.

View an Error Report

To view an error report using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **View an Error Report** on the next menu.
3. Select a report destination (**screen** or **transfer_directory**) from the selector screen.
4. Press **Tab** to select a report style, either **summary** or **detailed**.
5. Select values from the dialog screen to limit the scope of the error report. Use the default values in the dialog items to get a full report. If a null report is created, you have chosen a combination of options that are not found in the error log.

Error classes

Press **F4 (Esc + 4)** to list, **F9 (Esc + 9)** to select, and **Enter** to record selections. If you type in your selections, you cannot use lowercase letters. Only the following uppercase letters are supported:

- H — hardware
- S — software
- O — operator

Error types

Press **F4 (Esc + 4)** to list, **F9 (Esc + 9)** to select, and **Enter** to record selections.

- Permanent (PERM)
- Performance (PERF)
- Impending (PEND)
- Temporary (TEMP)
- Unknown (UNKN)

Resource classes

Press **F4 (Esc + 4)** to list, **F9 (Esc + 9)** to select, and **Enter** to record selections.

Resource names

Press **F4 (Esc + 4)** to list, **F9 (Esc + 9)** to select, and **Enter** to record selections.

Error IDs to include

Press **F4 (Esc + 4)** to list, **F9 (Esc + 9)** to select, and **Enter** to record selections.

Error IDs to exclude

Press **F4 (Esc + 4)** to list, **F9 (Esc + 9)** to select, and **Enter** to record selections.

Starting date and time

Set using the 'MMDDhhmmYY' format.

Ending date and time

Set using the 'MMDDhhmmYY' format.

Figure 11-2 shows an example of View an Error Report output.

ERROR_ID	TIMESTAMP	T	CL	RESOURCE_NAME	ERROR_DESCRIPTION
9DBCfDEE	1203125991	T	O	errdemon	Error logging turned on
192AC071	1202161691	T	O	errdemon	Error logging turned off
FCA960CE	1120114691	T	S	tok0	EXCESSIVE TOKEN-RING ERRORS
C14C511C	1120113291	T	H	scsi0	ADAPTER ERROR
C14C511C	1120113291	T	H	scsi0	ADAPTER ERROR
74533D1A	1120113191	U	H	SYSIOS	LOSS OF ELECTRICAL POWER
9DBCfDEE	1120113391	T	O	errdemon	Error logging turned on
74533D1A	1107094791	U	H	SYSIOS	LOSS OF ELECTRICAL POWER
C14C511C	1031070991	T	H	scsi0	ADAPTER ERROR
74533D1A	1031065091	U	H	SYSIOS	LOSS OF ELECTRICAL POWER
83F06558	0915220491	P	S	SYSPROC	SOFTWARE PROGRAM ABNORMALLY TERMINATED
AA8AB241	0914230491	T	O	OPERATOR	OPERATOR NOTIFICATION
9DBCfDEE	0913556891	T	O	errdemon	Error logging turned on
192AC071	0912456791	T	O	errdemon	Error logging turned off

Figure 11-2. Example of a Summary Error Report

This task can be invoked using command primitives. See “Error Report Command Primitives” on page 8-43 for information about the command primitives. The error log is up to 1 MB long and wraps when it is filled.

View an Error Report for a Single Sequence Number

Each error record contains a unique sequence number. This sequence number is sent to the network management station in the trap. To view an error report for a single sequence number using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **View an Error Report for a Single Sequence Number** on the next menu.
3. Select a report destination (**screen** or **transfer_directory**) from the selector screen.
4. Press **F4 (Esc + 4)** to select the sequence number from a pop-up list of all sequence numbers which are currently in the error log.

Figure 11-3 shows an example of a software error report. Figure 11-4 on page 11-9 shows an example of a hardware error report.

ERROR LABEL: SNMP_05
ERROR ID: 0FF3E351

Date/Time: Mon Nov 11 10:32:09
Sequence Number: 74529
Machine Id: 000000183000
Node Id: whip1
Error Class: S
Error Type: PERM
Resource Name: snmp

Error Description
SOFTWARE PROGRAM ERROR

Probable Causes
SOFTWARE PROGRAM

Failure Causes
SOFTWARE PROGRAM

Recommended Actions
CONTACT SERVICE REPRESENTATIVE
REPORT THE FOLLOWING

Detail Data
SYMPTOM CODE
5549 smux.tld interface-snmp 192
FILE NAME
snmp.config
REFERENCE CODE
423

Figure 11-3. Example of View an Error Report for a Single Sequence Number for a Software Error

```

ERROR LABEL:      SCSI_ERR1
ERROR ID:         0502F666

Date/Time:        Jun 19 22:29:51
Sequence Number:  95
Machine ID:       123456789012
Node ID:          host1
Class:            H
Type:             PERM
Resource Name:    scsi0
Resource Class:   adapter
Resource Type:    hscsi
Location:         00-08
VPD:
    Device Driver Level.....00
    Diagnostic Level.....00
    Display Message.....SCSI
    EC Level.....C25928
    FRU Number.....30F8834
    Manufacturer.....IBM97F
    Part Number.....59F4566
    Serial Number.....00002849
    ROS Level and ID.....24
    Read/Write Register Ptr.....0120
Error Description
ADAPTER ERROR

Probable Causes
ADAPTER
CABLE
CABLE TERMINATOR
DEVICE

Failure Causes
ADAPTER
CABLE LOOSE OR DEFECTIVE
DEVICE

Recommended Actions
PERFORM PROBLEM DETERMINATION PROCEDURES
CHECK CABLE AND ITS CONNECTIONS

```

```

Detail Data
SENSE DATA
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

```

Figure 11-4. Example of View an Error Report for a Single Sequence Number for a Hardware Error

This task can be invoked using command primitives. See “Error Report Command Primitives” on page 8-43 for information about the command primitives.

Clean the Error Log

Warning: The error log has a capacity of 1 MB and wraps when it is filled. Generally, the entries in the error log should never be deleted. However, entries for specific hardware failures should be deleted after any hardware replacement. Otherwise, any errors in the log from the failed hardware will continue to appear in error reports.

To delete specific error log entries using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Clean the Error Log** on the next menu.
4. Select appropriate days, resource classes, resource names, and error IDs from the dialog screen to limit deleting the entries for the failed hardware.

Remove entries older than this number of days

Type the number of days.

Remove entries for these Resource classes

Press **F4 (Esc + 4)** to list, **F9 (Esc + 9)** to select, and **Enter** to record the selections.

Remove entries for these Resource names

Press **F4 (Esc + 4)** to list, **F9 (Esc + 9)** to select, and **Enter** to record the selections.

Remove entries for these Error IDs

Press **F4 (Esc + 4)** to list, **F9 (Esc + 9)** to select, and **Enter** to record the selections.

No output is displayed from the Clean the Error Log menu item.

Use System and User Process Dump Facilities

There are three areas of the IBM 6611 to dump:

- Base operating system software
- User-process software
- Peer-capable adapter software

You can issue dump requests and view or gather the dumped output. From this menu, the operating system and user process memory can be dumped. Use the Adapter Debug Facility to dump the adapter code.

Figure 11-5 shows the menu screen for Use System and User Process Dump Facilities.

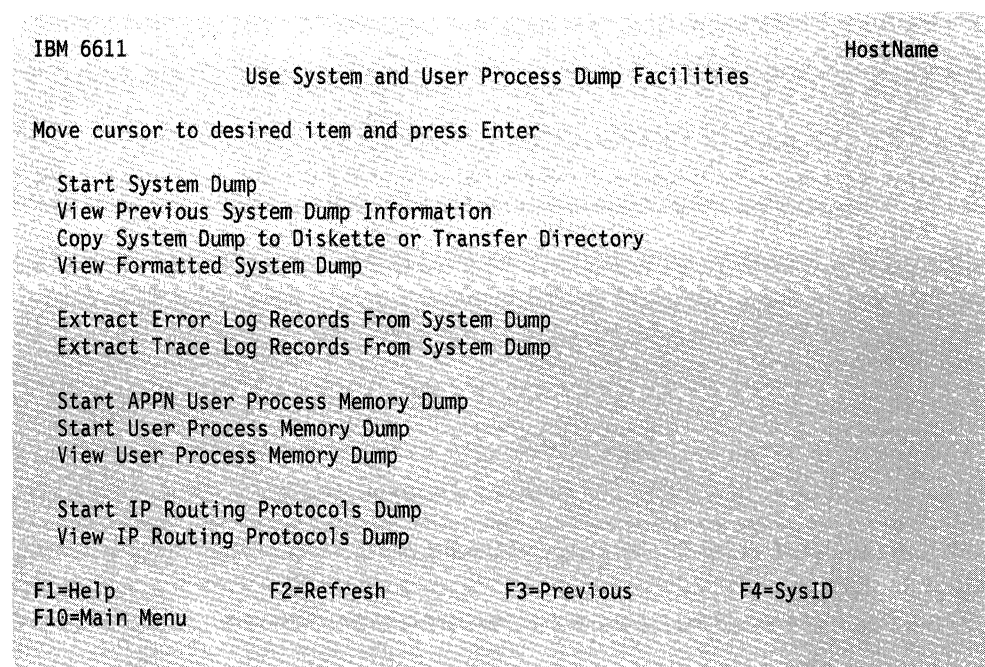


Figure 11-5. Use System and User Process Dump Facilities Menu

See these pages for more information about the individual menu items:

Start System Dump	11-12
View Previous System Dump Information	11-13
Copy System Dump to Diskette or Transfer Directory	11-14
View a Formatted System Dump	11-14
Extract Error Log Records From System Dump	11-15
Extract Trace Log Records From System Dump	11-15
Start APPN User Process Memory Dump	11-16
Start User Process Memory Dump	11-16
View User Process Memory Dump	11-17
Start IP Routing Protocols Dump	11-19
View IP Routing Protocols Dump	11-19

These tasks can be invoked using command primitives. See “Dump: System Command Primitives” on page 8-40 and “Dump: User Process Command Primitives” on page 8-42 for information about the dump command primitives.

Start System Dump

The IBM 6611 system dump copies selected system structures to the dump device when initiated by one of the following methods:

- An unexpected system halt occurs.
- The Reset button on the front panel is pressed with the key mode switch in Service position.
- The system dump is started using the System Manager.
- The system dump is started using command primitives issued from the fast-path environment, or the **rsh** or **rexec** commands.

The system dump originates in the dump device, */dev/hd7*. It can be copied to the transfer directory to be exported to a remote station. In this instance, there will be two copies of the same system dump. To save space in the transfer directory, please remove this dump as soon as possible.

To start a system dump using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use System and User Process Dump Facilities** on the next menu.
4. Select **Start System Dump** on the next menu.

You receive the following ARE YOU SURE message warning you of the results of dumping the IBM 6611:

ARE YOU SURE?

Executing this command will shut down your IBM 6611, stopping all the protocols and processes including the current System Manager session.
Press Enter to start the system dump.
Press Previous to cancel and return to the System Manager.

F1=Help F2=Refresh F3=Previous
F10=Main Menu

5. Press **Enter** to continue with dumping the IBM 6611.

You receive the following INFORMATION MESSAGE stating that your System Manager session is stopped:

INFORMATION MESSAGE

NOTE: This command needs to be run
outside of the System Manager.
Therefore the System Manager will exit
immediately before running this command.

Press Enter to proceed with the command.

Press Previous to cancel and return to
the System Manager.

F1=Help F2=Refresh F3=Previous
F10=Main Menu

6. Press **Enter** to start the dump process.

0c2 is displayed in the 3-digit display on the IBM 6611 during the dump process.
0c0 is displayed when the dump is complete.

7. Press the Reset button to restart the IBM 6611.

View Previous System Dump Information

The IBM 6611 dump device, */dev/hd7*, stores the last system dump taken. Certain statistical information about the last dump is also kept, such as, the date and time of the last dump, the number of blocks written, and the completion status.

To view previous system dump information using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use System and User Process Dump Facilities** on the next menu.
4. Select **View Previous System Dump Information** on the next menu.

If no dump is available, the following message is displayed:

No previous dumps recorded.

Figure 11-6 shows an example of View Previous System Dump Information output.

Device name:	/dev/hd7
Major device number:	10
Minor device number:	4
Size:	3461632 bytes
Date/Time:	Wed May 20 10:15:57 CDT 1992
Dump status:	0

Figure 11-6. Example of View Previous System Dump Information Output

Copy System Dump to Diskette or Transfer Directory

The system dump can be viewed while still residing in the dump device or it can be transferred out of the IBM 6611 to be viewed using a remote IBM 6611. You can place the system dump on a diskette or in the transfer directory.

To copy a system dump to a diskette or to the transfer directory using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use System and User Process Dump Facilities** on the next menu.
4. Select **Copy System Dump to Diskette or Transfer Directory** on the next menu.
5. Select a destination (**dump_diskette** or **transfer_directory**) from the selector screen.

Figure 11-7 shows an example of the status message you receive.

846+0 records in.
846+0 records out.

The system dump is copied to the transfer directory as: pd_system.dump

Figure 11-7. Example of Copy System Dump to Diskette or Transfer Directory Status Message

View a Formatted System Dump

The dump facility that formats the system dump interprets and formats the control structures in the base operating system and certain miscellaneous functions that are useful when examining a system dump.

To view a formatted system dump using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use System and User Process Dump Facilities** on the next menu.
4. Select **View a Formatted System Dump** on the next menu.
5. Select a destination for the formatted dump (**screen** or **transfer_directory**) from the selector screen.
6. Select a current dump location (**dump_device** or **transfer_directory**) from the selector screen.

If no dump is available, the following message is displayed:

There is not a dump in the dump device or
the dump device cannot be accessed.

7. Wait several minutes until the format processing stops.

Figure 11-8 on page 11-15 shows an example of View a Formatted System Dump output.

[TOP]

Reading in Symbols
SYSTEM STAT:

sysname: IBM 6611
nodename: u2
release: 1
version: 0
machine: 000268543100
time of crash: Wed May 20 10:15:57 1992
age of system: 4 day, 15 hr., 50 min.

SYSTEM VARIABLES

[MORE...10995]

Figure 11-8. Example of View a Formatted System Dump Output

Extract Error Log Records From System Dump

When the writing of an error log record to the error log on the fixed disk is interrupted by a system dump, the error log record is still available in the system dump.

To extract error log records from a system dump using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use System and User Process Dump Facilities** on the next menu.
4. Select **Extract Error Log Records From System Dump** on the next menu.

If there are no lost error records, the following message is displayed:

No error records available.

Extract Trace Log Records From System Dump

When the writing of a trace log record to the trace log on the fixed disk is interrupted by a system dump, the trace log record is still available in the system dump.

To extract trace log records from a system dump using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use System and User Process Dump Facilities** on the next menu.
4. Select **Extract Trace Log Records From System Dump** on the next menu.

If there are no lost trace records, the following message is displayed:

A trace session must be in progress when the system dump is invoked.

Start APPN User Process Memory Dump

This dump does not disrupt the APPN protocol. The dump output is displayed without causing you to restart the APPN protocol.

Note: To view the APPN dump, use “View User Process Memory Dump” on page 11-17.

This dump includes the current state of tasks, timers, protocols, and tables for the APPN routing protocol component. The dump is placed in the transfer directory.

To start a dump of the APPN routing protocol using the System Manager:

1. Log in using a controlling userid. See “Logging In to an IBM 6611” on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use System and User Process Dump Facilities** on the next menu.
4. Select **Start APPN User Process Memory Dump** on the next menu.

If the APPN routing protocols process is not started, the following message is displayed:

The APPN Routing Protocols Process is not currently running.
The APPN Routing Protocols Process cannot be dumped.
Please call IBM Service.

The example of View User Process Memory Dump in Figure 11-10 on page 11-18 shows an example of the status messages you receive for the APPN dump.

Start User Process Memory Dump

Any running user process in the IBM 6611 can be sent a signal telling it to dump its memory. This is a disruptive dump. Please call IBM service personnel for directions on restarting the process. The dump is automatically sent to the transfer directory, where it can be viewed or transferred to a remote node.

To start a memory dump of a user process using the System Manager:

1. Log in using a controlling userid. See “Logging In to an IBM 6611” on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use System and User Process Dump Facilities** on the next menu.
4. Select **Start User Process Memory Dump** on the next menu.
5. Select a process from the list in the selector screen.

6. You receive the following warning message:

ARE YOU SURE?

Executing a dump on a user process terminates the process. Dumping certain processes may hang your terminal or even bring down your IBM 6611, stopping the protocols and processes including the current System Manager Session.

Press Enter to continue
Press Previous to cancel and return to the System Manager.

F1=HelpF2=RefreshF3=Previous

F10=Main Menu

Press **Enter** to start the dump process.

Figure 11-9 shows an example of the status message you receive.

The dump has started.
When completed, the dump will be located in
the transfer directory referenced by the process name.

Figure 11-9. Example of Start User Process Memory Dump Status Output

View User Process Memory Dump

A user process memory dump is created automatically if the process crashes. To force a dump, you can issue a dump request using the Start User Process Memory Dump task in the System Manager or a command primitive. User process memory dumps are automatically placed in the transfer directory when the dump completes.

Note: If you want to view a large user process memory dump, it may take a long time to display the dump information.

To view a memory dump of a user process using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use System and User Process Dump Facilities** on the next menu.
3. Select **View User Process Memory Dump** on the next menu.
4. Select a process name from the list in the selector screen.

Figure 11-10 shows an example of View User Process Memory Dump output.

00000000:	06700003	000048A4	00004E0F	00002FE8	.p...H...N.../.
00000010:	2FF7DC80	00000000	00000000	0B000000	/.....
00000020:	0000283A	00000000	D00F22A8	0000D0B0	..(:....."
00000030:	00224000	D00F22A8	DEADBEEF	DEADBEEF	.."@..."
00000040:	DEADBEEF	00000000	00000000	01000000	
00000050:	30000000	40000000	200006A4	30000000	0...@... ..0...
00000060:	00000106	00000000	00000000	00000000	
00000070:	00000000	00000000	00000000	00000000	
00000080:	00000000	00000000	00000000	00000000	
00000090:	00000000	00000000	00000000	E01E0000	
000000A0:	40000707	40001A9A	40000666	007FFFFFFF	@...@...@.f....
000000B0:	007FFFFFFF	007FFFFFFF	007FFFFFFF	007FFFFFFF	
000000C0:	007FFFFFFF	007FFFFFFF	007FFFFFFF	007FFFFFFF	
000000D0:	007FFFFFFF	40000A0A	007FFFFFFF	007FFFFFFF	@.....
000000E0:	DEADBEEF	2FF7E018	2001C128	00000158	/... ..(.X
000000F0:	DEADBEEF	DEADBEEF	DEADBEEF	DEADBEEF	
00000100:	DEADBEEF	DEADBEEF	DEADBEEF	DEADBEEF	
00000110:	DEADBEEF	200528F0	200528D8	20052D20	(. .(. -
00000120:	00000000	20051A10	200533B8	200533C8	3. .3.
00000130:	20052D28	200534A8	20051A10	00000000	..-(.4.
00000140:	20052D36	20052078	000A0007	20052D39	..-6 . x.... -9
00000150:	00000000	00001000	2007C7C8	2007C7C8	
00000160:	00000000	00000000	00000000	00000000	
00000170:	00000000	00000000	00000000	00000000	
00000180:	00000000	00000000	00000000	00000000	

Figure 11-10. Example of View User Process Memory Dump Output

Start IP Routing Protocols Dump

This dump includes the current state of tasks, timers, protocols, and tables for the IP routing protocols component. The dump is placed in the transfer directory.

To start a dump of the IP routing protocols using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use System and User Process Dump Facilities** on the next menu.
4. Select **Start IP Routing Protocols Dump** on the next menu.

If the IP routing protocols process is not started, the following message is displayed:

```
The IP Routing Protocols Process is not currently running.  
The IP Routing Protocols Process cannot be dumped.  
Please call IBM Service.
```

Figure 11-11 shows an example of the status messages you receive.

```
IP routing protocols dump has started.  
The dump is being moved to transfer directory.  
IP routing protocols dump is now located in the transfer directory  
as pd_route_proto_dump.
```

Figure 11-11. Example of Start IP Routing Protocols Dump Status Messages

View IP Routing Protocols Dump

To view a dump of the IP routing protocols component using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use System and User Process Dump Facilities** on the next menu.
3. Select **View IP Routing Protocols Dump** on the next menu.

If the IP routing protocols process is not started, the following message is displayed:

```
The IP Routing Protocols dump could not be found in the transfer directory.  
You may need to start the IP Routing Protocols dump first.
```

Figure 11-12 shows an example of View IP Routing Protocols Dump output.

```
gated[10529] version 2.0.1.1.development memory dump on u2 at Wed May 20 20:18:22 1992
Started at Wed May 20 20:15:59 1992

Task State: <>

Tasks (6) and Timers:

  IF      Priority 10      Socket 7      RtProto Direct
        IF_Check      last: 20:17:57 next: 20:18:57 interval: 00:01:00

  RT      Priority 20
        RT_Age last: 20:17:57 next: 20:18:57 interval: 00:01:00

  ASPaths Priority 50

  KRT      Priority 60      Proto 255      Socket 20      RtProto Kernel RtBit 1 <Last>
        KRT_Timeout      <Absolute>

  Redirect      Priority 60

  SMUX.127.0.0.1 Priority 70      Port 199      RtProto MIB
        SMUX_Startup.127.0.0.1 last: 20:17:59 next: 20:18:59 interval: 00:01:00      <Absolute>

Timers without tasks:

  Time.Mark      last: 20:15:59 next: 20:25:59 interval: 00:10:00

Task to socket mapping:

  socket: 7      task: IF
  socket: 20      task: KRT

Task Blocks:
  Allocation size: 4096 Number of buckets: 32
```

Figure 11-12. Example of View IP Routing Protocols Dump Output

Use System Trace Facility

Figure 11-13 shows the menu screen for Use System Trace Facility.

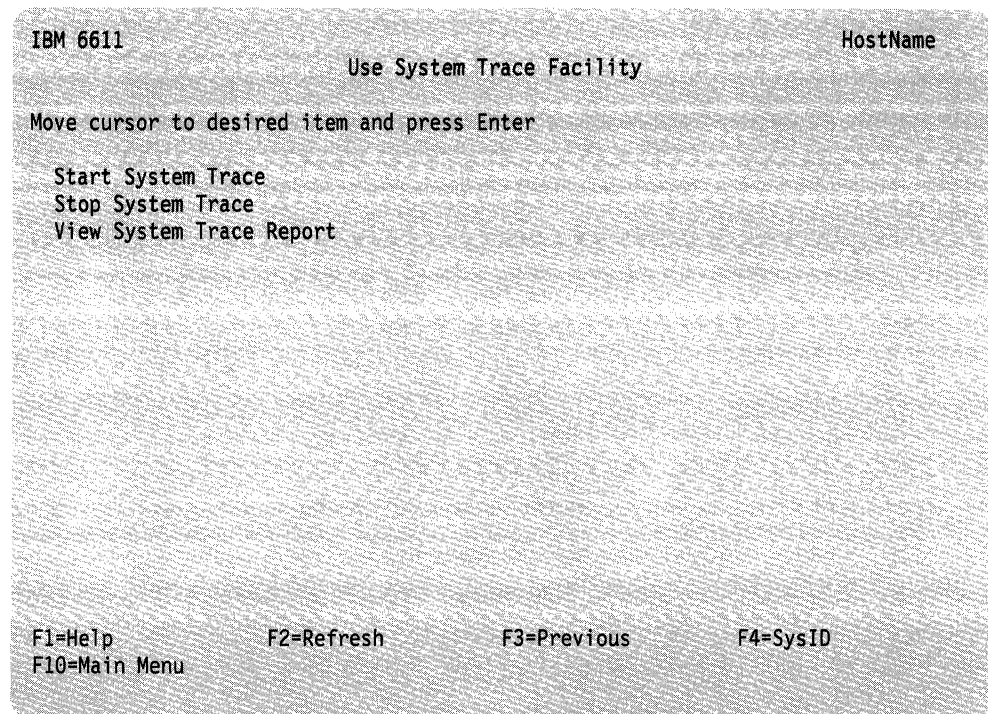


Figure 11-13. Use System Trace Facility Menu

The System Trace Facility is a system observation tool that captures a sequential flow of time-stamped system events. This facility is used by service personnel for problem determination. The trace goes to a 1 MB trace log that wraps when full. You can issue start and stop trace requests and generate and view trace reports.

See these pages for more information about the individual menu items:

Start System Trace	11-21
Stop System Trace	11-22
View System Trace Report	11-22

These tasks can be invoked using command primitives. See "Trace: System Command Primitives" on page 8-91 for information about the command primitives.

Start System Trace

Three buffer modes are available for tracing:

Circular buffer mode

Two collection buffers are maintained, and when one buffer becomes full, collection switches to the second buffer. The previous contents in the buffers are overwritten. The two buffers are written to the trace log when the trace is stopped.

Alternate buffer mode

Two collection buffers are maintained, and when one buffer becomes full, collection switches to the second buffer, while the contents of the first buffer are written to the trace log.

Single sweep buffer mode A single collection buffer is maintained. The trace data is written to the trace log. The trace is stopped when the buffer is filled, or when a trace stop request is received, whichever happens first.

To start a system trace using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use System Trace Facility** on the next menu.
4. Select **Start System Trace** on the next menu.
5. Select a trace mode, buffer size, and trace options from the dialog screen. The trace options include choosing trace event groups and individual trace event IDS to exclude from the event group or additional ones to include from other event groups.

Event groups to trace

Press **F4 (Esc + 4)** to list, **F9 (Esc + 9)** to select, and **Enter** to record selections.

Additional event IDs to trace

Press **F4 (Esc + 4)** to list, **F9 (Esc + 9)** to select, and **Enter** to record selections.

Event IDs to exclude from trace

Press **F4 (Esc + 4)** to list, **F9 (Esc + 9)** to select, and **Enter** to record selections.

Trace mode

Press **Tab** to select either **circular**, **single**, or **alternate**.

Trace buffer size

Define in bytes between 8192 and 524288. This value must be in decimal.

No output is displayed from the Start System Trace menu item.

Stop System Trace

To stop a system trace using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use System Trace Facility** on the next menu.
4. Select **Stop System Trace** on the next menu.

No output is displayed from the Stop System Trace menu item.

View System Trace Report

The system trace facility creates a formatted trace report. The report is sent either to the screen or to a file in the transfer directory. The report can include the whole trace log or can be limited by selecting specific event IDs to include or exclude and by including only trace records recorded between a specific start and end date and time.

To view a system trace report using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use System Trace Facility** on the next menu.

3. Select **View System Trace Report** on the next menu.
4. Select a report destination (**screen** or **transfer_directory**)
5. Select values from the dialog screen to limit the scope of the trace report.

IDs of events to include in report

Press **F4 (Esc + 4)** to list, **F9 (Esc + 9)** to select, and **Enter** to record selections

IDs of events to exclude in report

Press **F4 (Esc + 4)** to list, **F9 (Esc + 9)** to select, and **Enter** to record selections.

Starting date and time

Set using the 'MMDDhhmmssYY' format.

Ending date and time

Set using the 'MMDDhhmmssYY' format.

Let all the dialog items default to get a full report.

Figure 11-14 shows an example of View System Trace Report output.

```

Tue May 26 13:15:46 1992
System: IBM 6611 000013163000 Node: 3
Machine: 000013163000
Internet Address: 00000000 0.0.0.0

ID  PROCESS NAME  PID    I  SYSTEM CALL  ELAPSED  APPL  SYSCALL KERNEL  INTERRUPT

001 trace         10526                0.000000                TRACE ON channel 0                Tue May 26 13:15:47 1992
20F trace         10526                0.000055                unlock|      lock addr=11478                lock val=10526 pid=10526 return addr=15324
20E trace         10526                0.000065                lock|        lock addr=30C38                lock val=-1 pid=10526 return addr=887A8 flags=0000
20F trace         10526                0.000080                unlock|      lock addr=30C38                lock val=10526 pid=10526 return addr=85754
104 trace         10526                0.000096                return from system call
101 trace         10526      getppid      0.000112      getppid
147 trace         10526      getppid      0.000116                GETPPID
104 trace         10526      getppid      0.000120                return from getppid [8 usec]
101 trace         10526      kill        0.000137      kill
14E trace         10526      kill        0.000146                kill: signal SIGUSR1 to process 10269 trace
20E trace         10526      kill        0.000153                lock|        lock addr=30C30                lock val=-1 pid=10526 return addr=361E8 flags=0000
119 trace         10526      kill        0.000183                KERN_SENDSIGNAL hookdata 0000                00002B1D 0000001E 00000000 00000000 00000000
11F trace         10526      kill        0.000208                set on ready queue trace 10269
11F trace         10526      kill        0.000238                set on ready queue trace 10526
106 trace         10269                0.000249                dispatch trace 10269
200 trace         10269                0.000261                resume trace
20F sysmon        7006                0.145551                unlock|      lock addr=56E8248                lock val=7006 pid=7006 return addr=9BEA4
20E sysmon        7006                0.145576                lock|        lock addr=56E8248                lock val=-1 pid=7006 return addr=9BE28 flags=0000
20F sysmon        7006                0.145590                unlock|      lock addr=56E8248                lock val=7006 pid=7006 return addr=9BEA4
20E sysmon        7006                0.145710                lock|        lock addr=30C38                lock val=-1 pid=7006 return addr=893D4 flags=0000
20F sysmon        7006                0.145769                unlock|      lock addr=30C38                lock val=7006 pid=7006 return addr=9A3B4
100 sysmon        7006                0.145841                DATA ACCESS PAGE FAULT
184 sysmon        7006                0.145869                VMM lockmiss:      V.S=02DD.345A ppage=03C1
                        persistent_storage journaled system_segment modified
200 sysmon        7006                0.145895                resume sysmon
403 kproc         514      1      3.587969                (0010,0000,0000) rs offlevel ret 0 @ 2315
103 kproc         514      1      3.587981                return from slih [121 usec]
200 kproc         514      1      3.587988                resume IDLE
100 kproc         514                3.589197                I/O INTERRUPT
102 kproc         514      1      3.589214                slih clock [1354 usec]
234 kproc         514      1      3.589236                KERN_PROF 7630 [10007 usec]
103 kproc         514      1      3.589315                return from slih [100 usec]
10C kproc         514      1      3.589347                DISPATCH IDLE PROCESS
200 kproc         514      1      3.589350                resume IDLE
100 kproc         514                3.599195                I/O INTERRUPT
102 kproc         514      1      3.599212                slih clock [9997 usec]
234 kproc         514      1      3.599232                KERN_PROF 7630 [9995 usec]
103 kproc         514      1      3.599296                return from slih [84 usec]
10C kproc         514      1      3.599321                DISPATCH IDLE PROCESS

```

Figure 11-14. Example of View System Trace Report Output

Use Special User Process Traces

Several of the user processes and protocols have special traces designed specifically to help debug problems in those processes. The output from these traces is shown in this section. However, the details of the trace data are not explained. The trace data is obtained for service personnel to use.

Figure 11-15 shows the menu screen for Use Special User Process Traces.

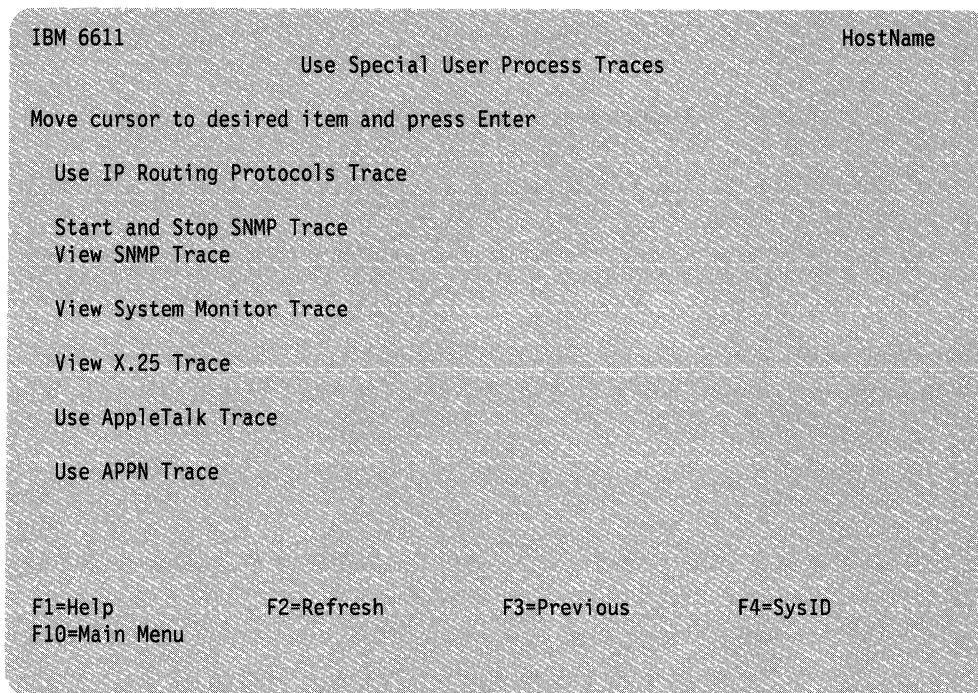


Figure 11-15. Use Special User Process Traces Menu

See these pages for more information about the individual menu items:

Use IP Routing Protocols Trace	11-25
Start and Stop SNMP Trace	11-28
View SNMP Trace	11-28
View System Monitor Trace	11-29
View X.25 Trace	11-30
Use AppleTalk Trace	11-31
Use APPN Trace	11-34

These tasks can be invoked using command primitives. See "Trace: User Process Command Primitives" on page 8-94 for information about the command primitives.

Use IP Routing Protocols Trace

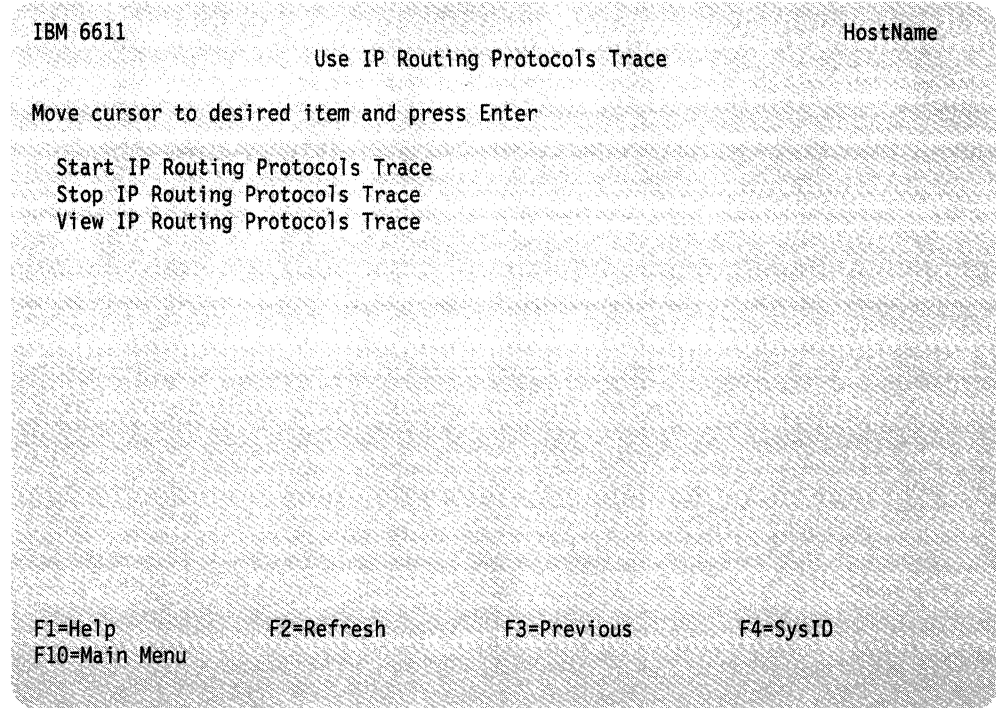


Figure 11-16. Use IP Routing Protocols Trace Menu

The IP Routing Protocols Trace is designed to facilitate solving problems with the IP Routing Protocols software. The trace facility allows you to select from a long list of trace options. This trace should only be started by service personnel who are knowledgeable about the IP Routing Protocol process. The trace output is gathered in the transfer directory. Figure 11-16 shows the menu screen for Use IP Routing Protocols Trace. See these pages for more information about the individual menu items:

Start IP Routing Protocols Trace	11-25
Stop IP Routing Protocols Trace	11-26
View IP Routing Protocols Trace	11-26

Start IP Routing Protocols Trace: The IP Routing Protocols Trace has a large group of options available. These trace options are turned either ON or OFF.

To start a trace of the IP Routing Protocols using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use Special User Process Traces** on the next menu.
4. Select **Use IP Routing Protocols Trace** on the next menu.
5. Select **Start IP Routing Protocols Dump** on the next menu.

6. Press **Tab** to select either **yes** or **no** on the dialog screen to turn on or off each of the following trace options:

- Do you wish to time stamp all trace data?
- Output a message to the trace log file every 10 minutes?
- Trace all options listed below?
- Internal and external errors and changes to IP Routing Protocols route table
- Internal errors and informational messages
- External errors
- Task scheduling, signal handling, and packet reception
- Timer scheduling
- Objects found by the lex analyzer
- The tokens the parser recognizes
- Tokens read from the configuration file to verify they were parsed correctly
- Protocol state machine transitions when used with BGP, EGP or OSPF
- Changes to the IP routing protocols route table
- Changes to the system routing table
- BGP packets sent and received
- EGP packets sent and received
- RIP packets sent and received
- HELLO packets sent and received
- ICMP packets sent and received
- SNMP packets sent and received
- OSPF packets sent and received
- Contents of protocol packets
- Policy list allocation.

You receive the following message after starting the IP Routing Protocols Trace:

The IP routing protocol is being restarted with traces turned on.

The trace output is collected in `pd_route_proto.trc` in the transfer directory.

Stop IP Routing Protocols Trace: To stop a trace of the IP Routing Protocols using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use Special User Process Traces** on the next menu.
4. Select **Use IP Routing Protocols Trace** on the next menu.
5. Select **Stop IP Routing Protocols Trace** on the next menu.

No output is displayed from the Stop IP Routing Protocols Trace menu item.

View IP Routing Protocols Trace: To view a trace of the IP Routing Protocols using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use Special User Process Traces** on the next menu.
3. Select **Use IP Routing Protocols Trace** on the next menu.
4. Select **View IP Routing Protocols Trace** on the next menu.

Figure 11-17 shows an example of View IP Routing Protocols Trace output.

```
May 29 20:34:00 Tracing flags enabled: general kernel
May 29 20:34:00
May 29 20:34:00 Start gated[8359] version 2.0.1.1.development built Wed May 27 02:26:51 EDT 1992
May 29 20:34:00
May 29 20:34:00 if_ifread: interface name lo0 address #1 lo0
May 29 20:34:00
May 29 20:34:00 if_ifread: interface name lo0 address 127.0.0.1
May 29 20:34:00 if_rtadd: ADD route for interface lo0 127.0.0.1/255
ADD    127.0.0.1      gw 127.0.0.1      Direct  pref  0 metric 0 lo0 <NoAge Refresh NoAdvise Host Active Retain>
ADD    127           gw 127.0.0.1      Direct  pref  0 metric 0 lo0 <NoAge Refresh NoAdvise Int Active Retain Reject>
May 29 20:34:00 if_ifread: interface lo0: up addr 127.0.0.1 metric 0 index 1 preference 0
May 29 20:34:00 if_ifread: interface lo0: net 127 netmask 255
May 29 20:34:00 if_ifread: interface lo0: refcount 1 mtu 1536 flags <Up Loopback Interface NoAge>
May 29 20:34:00 if_ifread: interface lo0: route: installed
May 29 20:34:00
May 29 20:34:00 if_ifread: interface name tr0 address #2 tr0
May 29 20:34:00
May 29 20:34:00 if_ifread: interface name tr0 address 17.17.17.2
May 29 20:34:00
May 29 20:34:00 if_rtadd: ADD route for interface tr0 17.17.17.2/255.255.255
ADD    17.17.17      255.255.255 gw 17.17.17.2 Direct  pref  0 metric 0 tr0 <NoAge Refresh Subnet Int Active Retain>
ADD    17            gw 17.17.17.2 Direct  pref  0 metric 0 tr0 <NoAge Refresh NotInstall Int Active>
May 29 20:34:00 if_ifread: interface tr0: up addr 17.17.17.2 metric 0 index 2 preference 0
May 29 20:34:00 if_ifread: interface tr0: broadaddr 17.17.17.255
May 29 20:34:00 if_ifread: interface tr0: net 17 netmask 255
May 29 20:34:00 if_ifread: interface tr0: subnet 17.17.17 subnetmask 255.255.255
May 29 20:34:00 if_ifread: interface tr0: refcount 1 mtu 1492 flags <Up Broadcast Subnet Interface>
May 29 20:34:00 if_ifread: interface tr0: route: installed
May 29 20:34:00
May 29 20:34:00 rt_close: 4 routes proto IF
May 29 20:34:00
May 29 20:34:00 krt_get_maxpacket: Maximum kernel receive/send packet size is 65535
May 29 20:34:00
May 29 20:34:00
May 29 20:34:00 krt_rtread: Initial routes read from kernel:
May 29 20:34:00 KRT RTINFO type GET(4)flags UP(1) error 0
May 29 20:34:00 KRT RTINFO dst 17.17.17 gateway 17.17.17.2 netmask 255.255.255
May 29 20:34:00
ADD    17.17.17      255.255.255 gw 17.17.17.2 Kernel  pref 255 metric 0 tr0 <Refresh NoAdvise Subnet Int>
RELEASE 17.17.17      255.255.255 gw 17.17.17.2 Kernel  pref 255 metric 0 tr0 <Refresh NoAdvise Subnet Int Release>
May 29 20:34:00 KRT RTINFO type GET(4)flags UP HOST(5) error 0
May 29 20:34:00 KRT RTINFO dst 127.0.0.1 gateway 127.0.0.1
May 29 20:34:00
ADD    127.0.0.1      gw 127.0.0.1      Kernel  pref 255 metric 0 lo0 <Refresh NoAdvise Host>
RELEASE 127.0.0.1      gw 127.0.0.1      Kernel  pref 255 metric 0 lo0 <Refresh NoAdvise Host Release>
May 29 20:34:00 rt_close: 4 routes proto KRT
May 29 20:34:00
May 29 20:34:02 snmp_connect: CONNECT: smux_init: systemError [join_tcp_server failed: Connection refused]
(Connection
ref
```

Figure 11-17. Example of View IP Routing Protocols Trace Output

Start and Stop SNMP Trace

The simple network management protocol (SNMP) set of processes has a trace facility designed to help solve problems with the SNMP software. This trace facility should only be used by service personnel who are knowledgeable about the SNMP processes.

The SNMP trace facility has several trace options from which to select. The different trace options turn *on* or *off* tracing for a given SNMP process.

To start and stop SNMP traces using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use Special User Process Traces** on the next menu.
4. Select **Start and Stop SNMP Trace** on the next menu.
5. Press **Tab** to select **start** or **stop** on the dialog screen to either start or stop the selected trace option.
6. Press **F4 (Esc + 4)** to list the trace options on the dialog screen. Select one of SNMP processes by pressing **Enter** on the selected process:
 - snmpd
 - smux.cfgd
 - smux.dlsd
 - smux.pppd
 - smux.r66d
 - smux.rs960d
 - smux.t1d
 - smux.trapd.
7. Return to the dialog screen to select an additional SNMP process which can start or stop a trace.

Figure 11-18 shows an example of Start and Stop SNMP Trace output.

Trace started on process smux.cfgd

Figure 11-18. Example of Start and Stop SNMP Trace Output

View SNMP Trace

To view the output of the SNMP trace using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use Special User Process Traces** on the next menu.
3. Select **View SNMP Trace** on the next menu.
4. Select the SNMP process whose trace you want to view from the selector screen.

Figure 11-19 shows an example of SNMP Trace output.

05/31 16:43:11 (09691) cfgd	- refreshing shared interface table...
05/31 16:43:15 (09691) cfgd	- reconfiguring snmp subsystem...
05/31 16:43:15 (09691) cfgd	- refreshing shared interface table...
05/31 16:43:24 (09691) cfgd	- MSG TO SYSMON: sysmon: start snmpd
05/31 16:43:24 (09691) cfgd	- MSG TO SYSMON: sysmon: start smux.trapd
05/31 16:43:24 (09691) cfgd	- MSG TO SYSMON: sysmon: start smux.r66d
05/31 16:43:24 (09691) cfgd	- MSG TO SYSMON: sysmon: start smux.rs960d
05/31 18:30:24 (09691) cfgd	- terminating due to SIGTERM signal
05/31 18:30:25 (09691) cfgd	- shared interface table disconnected
05/31 18:30:25 (09691) cfgd	- cfgd is terminating
05/31 19:01:27 (06358) cfgd	- refreshing shared interface table...
05/31 19:02:28 (06358) cfgd	- reconfiguring snmp subsystem...
05/31 19:02:28 (06358) cfgd	- refreshing shared interface table...
05/31 19:03:04 (06358) cfgd	- MSG TO SYSMON: sysmon: start snmpd
05/31 19:03:04 (06358) cfgd	- MSG TO SYSMON: sysmon: start smux.trapd
05/31 19:03:04 (06358) cfgd	- MSG TO SYSMON: sysmon: start smux.r66d
05/31 19:03:04 (06358) cfgd	- MSG TO SYSMON: sysmon: start smux.rs960d
05/31 19:06:37 (06358) cfgd	- terminating due to SIGTERM signal
05/31 19:06:37 (06358) cfgd	- shared interface table disconnected
05/31 19:06:37 (06358) cfgd	- cfgd is terminating
05/31 19:14:47 (09967) cfgd	- refreshing shared interface table...
05/31 19:16:08 (09967) cfgd	- reconfiguring snmp subsystem...
05/31 19:16:09 (09967) cfgd	- refreshing shared interface table...
05/31 19:16:43 (09967) cfgd	- MSG TO SYSMON: sysmon: start snmpd
05/31 19:16:43 (09967) cfgd	- MSG TO SYSMON: sysmon: start smux.trapd
05/31 19:16:43 (09967) cfgd	- MSG TO SYSMON: sysmon: start smux.r66d
05/31 19:16:43 (09967) cfgd	- MSG TO SYSMON: sysmon: start smux.rs960d
05/31 19:21:24 (09967) cfgd	- terminating due to SIGTERM signal
05/31 19:21:24 (09967) cfgd	- shared interface table disconnected
05/31 19:21:24 (09967) cfgd	- cfgd is terminating
05/31 19:26:26 (07394) cfgd	- refreshing shared interface table...
05/31 19:27:24 (07394) cfgd	- reconfiguring snmp subsystem...
05/31 19:27:24 (07394) cfgd	- refreshing shared interface table...
05/31 19:27:39 (07394) cfgd	- MSG TO SYSMON: sysmon: start snmpd
05/31 19:27:39 (07394) cfgd	- MSG TO SYSMON: sysmon: start smux.trapd
05/31 19:27:39 (07394) cfgd	- MSG TO SYSMON: sysmon: start smux.r66d
05/31 19:27:39 (07394) cfgd	- MSG TO SYSMON: sysmon: start smux.rs960d
05/31 19:29:21 (07394) cfgd	- terminating due to SIGTERM signal
05/31 19:29:21 (07394) cfgd	- shared interface table disconnected
05/31 19:29:21 (07394) cfgd	- cfgd is terminating

Figure 11-19. Example of View SNMP Trace Output

View System Monitor Trace

The system monitor is a major process in the IBM 6611 software. It monitors all the system components, starting and stopping them when it determines the need. It also monitors the file space and deletes unnecessary files from the transfer directory and files in other parts of the IBM 6611 when they reach a predetermined size. The system monitor trace is a log of all of its activity. The trace is always running. The trace file is truncated when it reaches a certain size. This trace is useful for debugging system problems.

To view the system monitor trace log using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use Special User Process Traces** on the next menu.
3. Select **View System Monitor Trace** on the next menu.

Figure 11-20 shows a sample of the system monitor trace log.

```
Jul 25 08:40:13 pppsysmond: /etc/ppp/pppsysmond : to0 LinkQuality is Good before But Look Bad Now
Jul 25 08:40:13 to0: pppsysmond : Jul 25 08:40:13 proto 8021 to0 is Closed ..., preSt=Open, curEv=Terminate, preEv=St atRequest
Jul 25 08:40:13 configd: get data from SYSMON
Jul 25 08:40:13 configd: pppsysmond : Jul 25 08:40:13 :proto 8021 to0 is Closed ..., preSt=Open, curEv=Terminate, preEv=StatRequest
Jul 25 08:40:13 configd:
Jul 25 08:40:14 to0: Jul 25 08:40:14 : **** A ppp Daemon, ipcp to0 exited, pid=8677
Jul 25 08:40:14 configd: get data from SYSMON
Jul 25 08:40:14 configd: Jul 25 08:40:14 : **** A ppp Daemon, ipcp to0 exited, pid=8677
Jul 25 08:40:14 configd:
Jul 25 08:40:35 pppsysmond: /etc/ppp/pppsysmond : to0 LinkQuality is Bad before And Look still Bad now
Jul 25 09:00:04 performing action 'frob snmpd' for socket
Jul 25 09:00:23 pppsysmond: /etc/ppp/pppsysmond : to0 LinkQuality is Bad before And Look still Bad now
```

Figure 11-20. Example of System Monitor Trace Log

View X.25 Trace

The X.25 protocol has a trace log that can be viewed when problems arise with the X.25 system component. The trace is always running and is truncated appropriately.

To view the X.25 trace using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use Special User Process Traces** on the next menu.
3. Select **View X.25 Trace** on the next menu.

Figure 11-21 shows a sample of the X.25 trace output.

```
crack_args: daemon_action_flg is 4
crack_args: daemon_action_flg is 4
test debug -540405504
init_structs: number = 0
init_structs: number = 1
init_structs: number = 2
init_structs: number = 3
init_structs: number = 4
init_structs: number = 5
init_structs: number = 6
after init_structs
init_sock: after unlink
init_sock: after socket
init_sock: after bind
init_sock: after listen
after init_sock
action_io: going into loop now
```

Figure 11-21. Example of X.25 Trace Output

Use AppleTalk Trace

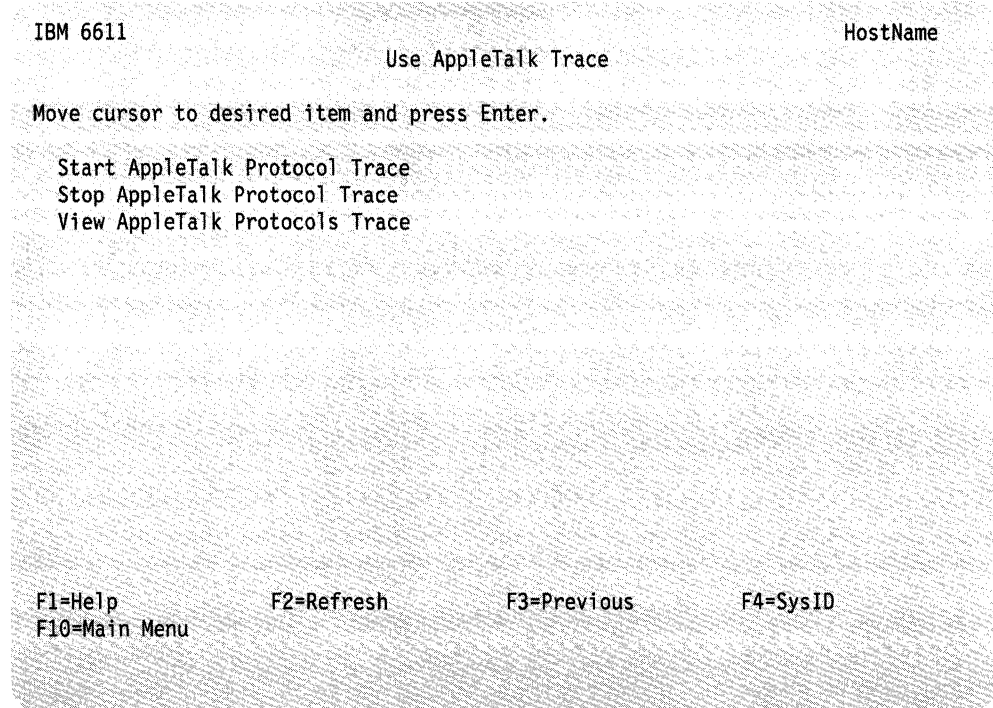


Figure 11-22. Use AppleTalk Trace Menu

The AppleTalk Protocols Trace is designed to facilitate solving problems with the AppleTalk software. The trace facility allows you to select from a list of trace options. This trace should be started only by service personnel who are knowledgeable about the AppleTalk Protocol process. The trace output is gathered in the transfer directory. Figure 11-22 shows the menu screen for Use AppleTalk Trace. See these pages for more information about the individual menu items:

Start AppleTalk Protocol Trace	11-31
Stop AppleTalk Protocol Trace	11-32
View AppleTalk Protocol Trace	11-32

Start AppleTalk Protocol Trace: The AppleTalk Protocols Trace has several trace options. These trace options are turned either ON or OFF.

To start a trace of the AppleTalk Protocols using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use Special User Process Traces** on the next menu.
4. Select **Use AppleTalk Trace** on the next menu.
5. Select **Start AppleTalk Protocol Trace** on the next menu.
6. Press **Tab** to select either **yes** or **no** on the dialog screen to turn on or off each of the following trace options:
 - Trace all protocols and miscellaneous flags
 - Trace ZIP protocol

- Trace ATP protocol
- Trace RTMP protocol
- Trace NBP protocol
- Trace all non-protocol flags

You receive the following message after starting the AppleTalk Protocols Trace:

The AppleTalk routing protocol is being restarted with traces turned on

The trace output will be collecting in file pd_appletalk.trc
in the transfer directory

Command completed successfully

Stop AppleTalk Protocol Trace: To stop a trace of AppleTalk Protocols using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use Special User Process Traces** on the next menu.
4. Select **Use AppleTalk Trace** on the next menu.
5. Select **Stop AppleTalk Protocol Trace** on the next menu.

No output is displayed from the Stop AppleTalk Protocol Trace menu item.

View AppleTalk Protocol Trace: To view a trace of the AppleTalk Protocols using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use Special User Process Traces** on the next menu.
3. Select **Use AppleTalk Trace** on the next menu.
4. Select **View AppleTalk Protocol Trace** on the next menu.

Figure 11-23 shows an example of View AppleTalk Protocol Trace output.

```
tracing to "/tmp/hold/transfer/pd_appletalk.trc" startedstarting trace file /tmp/h
old/transfer/pd_appletalk.trc msgflg = 0xffff
adding interface tel at net table slot 0
multicast address: '09:00:07:99:88:77'
address sent by nap to card
RTMP: adding net 222: 222 hopcnt 0 nexthop 200
writing to routing socket ADD net=222.222
writing to routing socket ADD net=222.222
SOCKET: local route added
added net 0.de bzone
multicast address: 09:00:07:00:00:28
starting socket for port 1
starting socket for port 3
starting socket for port 6
starting socket for port 2
RTMP_SEND: sending RTMP for net 222.222
RTMP_SEND: sending packet 16
output DDP PACKET received: len = 29 dnet = 0, snet = 222 dnode = 255, snode = 200
net range = 222 to 222, dst= 0
net range = 222 to 222, dst= 0
packet sent
zip_send: for interface"0"
RTMP_SEND: sending RTMP for net 222.222
RTMP_SEND: sending packet 16
output DDP PACKET received: len = 29 dnet = 0, snet = 222 dnode = 255, snode = 200
, dsock = 1, ssock = 1, proto = rtmp data
Net = 222 Node ID len = 8 Node ID = 200
net range = 222 to 222, dst= 0
net range = 222 to 222, dst= 0
packet sent
zip_send: for interface"0"
rtmp_age
```

Figure 11-23. Example of View AppleTalk Protocol Trace Output

Use APPN Trace

Figure 11-24 shows the menu screen for Use APPN Trace.

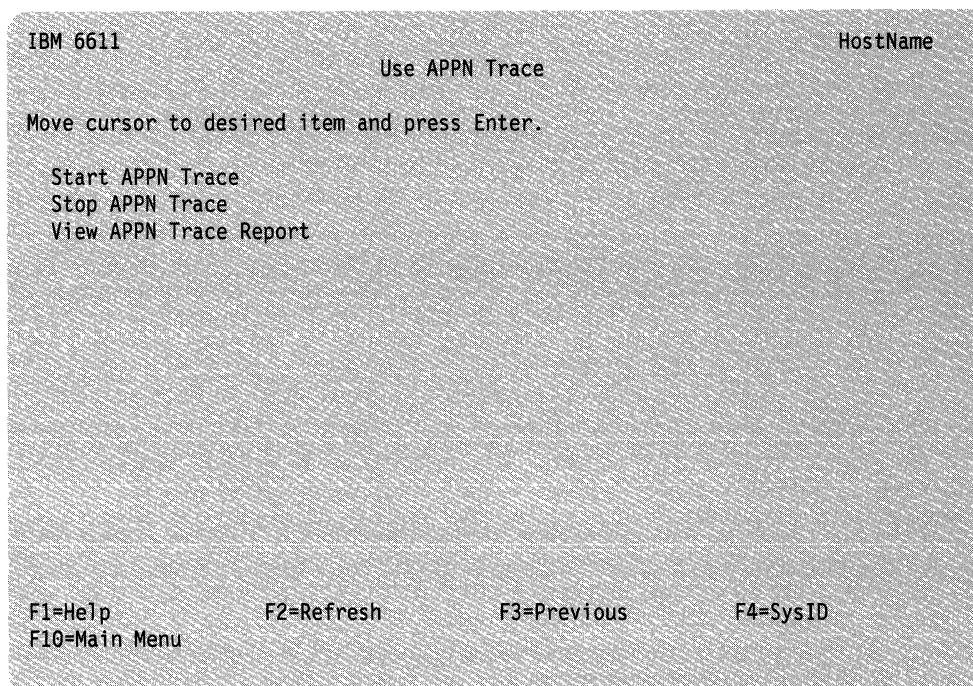


Figure 11-24. Use APPN Trace Menu

The APPN Trace is designed to facilitate solving problems with the APPN software. The trace facility allows you to select from a long list of trace options. This trace should only be started by service personnel who are knowledgeable about the APPN process. The trace output is gathered in the transfer directory.

APPN trace is an enhanced system trace. The APPN trace allows both the system trace data and the APPN trace data to be collected simultaneously. Figure 11-24 shows the menu screen for Use APPN Trace. See these pages for more information about the individual menu items:

Start APPN Trace	11-34
Stop APPN Trace	11-35
View APPN Trace Report	11-35

Start APPN Trace: The APPN Trace has a large group of options available. These trace options are turned either ON or OFF.

To start a trace of the IP Routing Protocols using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use Special User Process Traces** on the next menu.
4. Select **Use APPN Trace** on the next menu.
5. Select **Start APPN Trace** on the next menu.
6. Type the appropriate information in to the entry fields:

- Event groups to trace (default is system activity)
 - Additional event ids to trace
 - Event ids to exclude from trace
 - Trace mode
 - Trace buffer size in bytes (8K to 512K)
7. Press **Tab** to select either **yes** or **no** on the dialog screen to turn on or off each of the following trace options:

APPN Trace Flags

- Turn All Trace Filter Flags On
- Trace Process Management
- Trace process to process communication
- Trace locking
- Trace miscellaneous tower activities
- Trace I/O to and from the system
- Trace storage management
- Trace Queue data type management
- Trace Table data type management
- Trace buffer management
- Trace Configuration control
- Trace timer service
- Trace service provider management
- Trace interprocess message segmenting
- Trace control of processes outside scope of tower
- Trace monitoring of processes, services, towers
- Trace distributed environment control

No output message is displayed after starting APPN trace.

Stop APPN Trace: To stop a trace of APPN using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use Special User Process Traces** on the next menu.
4. Select **Use APPN Trace** on the next menu.
5. Select **Stop APPN Trace** on the next menu.

No output is displayed from the Stop APPN Trace menu item.

View APPN Trace Report: To view a trace of the APPN Protocols using the System Manager:

APPN trace is an enhanced system trace. The APPN trace allows both the system trace data and the APPN trace data to be view simultaneously.

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use Special User Process Traces** on the next menu.
3. Select **Use APPN Trace** on the next menu.
4. Select **View APPN Trace Report** on the next menu.

Figure 11-25 shows an example of View APPN Trace Report output.

ID	ELAPSED_SEC	DELTA_MSEC	APPL	SYSCALL	KERNEL	INTERRUPT
EGPE trace: Pid=00201010 Lock_p= 60000044			Process name=testx4u			unlock
EGPE trace: Pid=00201010 Lock_p= 6002B194 Mode= Exclusive			Process name=testx4u			lock
EGPE trace: Pid=00201010 Lock_p= 6002B194 Mode= Shared			Process name=testx4u			lock
EGPE trace: Pid=00201010 Lock_p= 6002B194			Process name=testx4u			unlock
EGPE trace: Pid=00201010 T=6002BDF8 Row @= 00000000			Process name=testx4u			Tfindk
EGPE trace: Pid=00201010 T=6002BDF8 Row @= 00000000			Process name=testx4u			Tfindk
EGPE trace: Pid=00201010 T=6002BDF8 Row @= 00000000			Process name=testx4u			Tfindk
EGPE trace: Pid=00201010 T=6002BDF8 Row @= 00000000			Process name=testx4u			Tfindk
EGPE trace: Pid=00201010 Lock_p= 6002B194 Mode= Exclusive			Process name=testx4u			lock
EGPE trace: Pid=00201010 Lock_p= 6002B194 Mode= Shared			Process name=testx4u			lock
EGPE trace: Pid=00201010 T=6002C458 Row @= 6001D200			Process name=testx4u			Tfindk
EGPE trace: Pid=00201010 Lock_p= 6002B194			Process name=testx4u			unlock
EGPE trace: Pid=00201010 Lock_p= 6002B194			Process name=testx4u			unlock
EGPE trace: Pid=00201010 Lock_p= 6002B194			Process name=testx4u			unlock
EGPE trace: Pid=00201010 Serv= TEST Rsp Corr=00000001 Rsp Pid=00201010 Rsp Qn=0			Process name=testx4u			PEstart_service_monitor
EGPE trace: Pid=00201010 Lock_p= 6002B194 Mode= Exclusive			Process name=testx4u			lock
EGPE trace: Pid=00201010 T=6002C458 Row @= 6001D200			Process name=testx4u			Tfindk
EGPE trace: Pid=00201010 T=6002B9B8 Row @= 60031E78			Process name=testx4u			Tfindk
EGPE trace: Pid=00201010 Addr= 60030558 Size= 00000084			Process name=testx4u			Mget
EGPE trace: Pid=00201010 Pid= 00201010 Qn= 0 Data_p= 60030558 Data= 00003402 , 00000000			Process name=testx4u			PQenq
EGPE trace: Pid=00201010 T=6002C018 Row @= 00000000			Process name=testx4u			Tfindk
EGPE trace: Pid=00201010 Addr= 6002E178 Size= 00000028			Process name=testx4u			Mget
EGPE trace: Pid=00201010 Addr= 6002D118 Size= 00000134			Process name=testx4u			Mget
EGPE trace: Pid=00201010 Addr= 6002D118 Size= 00000134			Process name=testx4u			Mget_clr

Figure 11-25. Example of View APPN Trace Report Output

Use Adapter Debug Facility

Figure 11-26 shows the menu screen for Use Adapter Debug Facility.

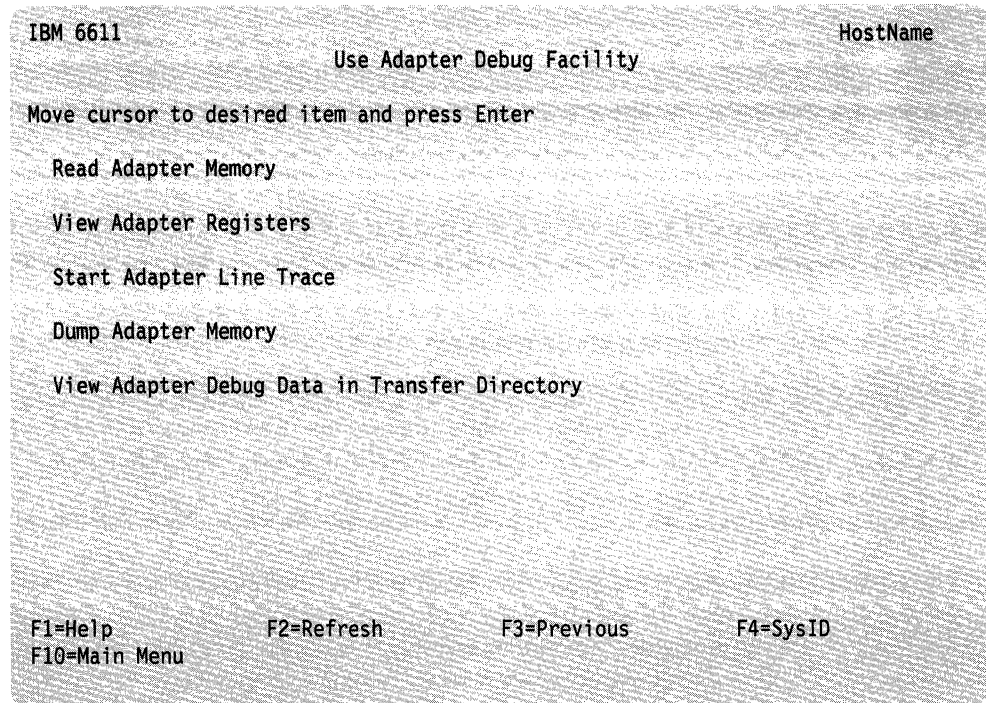


Figure 11-26. Use Adapter Debug Facility Menu

This facility is used with these peer-capable adapters:

- Token-Ring Network 16/4 Adapter
- Ethernet Adapter
- EIA 422/449 Serial Adapter
- V.35/V.36 Serial Adapter.

Table 11-1 explains the methodology for the internal names for these adapters. These names are used throughout this Adapter Debug Facility.

Table 11-1. Adapter Name Table

Adapter Name	Internal Adapter Name
Token-Ring Network 16/4 Adapter	trtya#
Ethernet Adapter	entya#
EIA 422/449 Serial Adapter	t1tya#
V.35/V.36 Serial Adapter	t1tya#

The number sign (#) sign is a number from 0 to 6. The number corresponds to the order of that particular adapter type as it is located in the IBM 6611. For example, **entya0** corresponds to the first Ethernet Adapter and **t1tya1** corresponds to the second serial adapter.

This Adapter Debug Facility is not used in normal operation of the IBM 6611. It is used by service representatives to troubleshoot problems with the peer-capable

adapter software. The adapter line trace also can be used to determine data that flows into and out of the IBM 6611.

See these pages for more information about the individual menu items:

Read Adapter Memory	11-38
View Adapter Registers	11-39
Start Adapter Line Trace	11-39
Dump Adapter Memory	11-41
View Adapter Debug Data in Transfer Directory	11-41

These tasks can be invoked using command primitives. See “Adapter Debug Facility Command Primitives” on page 8-10 for information about the command primitives.

Read Adapter Memory

To read the adapter memory using the System Manager:

1. Log in using a controlling userid. See “Logging In to an IBM 6611” on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use Adapter Debug Facility** on the next menu.
4. Select **Read Adapter Memory** on the next menu.
5. Select the destination for the adapter memory output (**screen** or **transfer_directory**) from the selector screen.
6. Select an adapter from the selector screen. See Table 11-1 on page 11-37 for an explanation of the adapter name.
7. Select or provide the appropriate values on the dialog screen to specify what to read from the adapter memory:
 - Unit to read by
 - word 4 bytes
 - short 2 bytes
 - bytes 1 byte
 - Address or symbol to start read

The address can be any hexadecimal number or known symbol. If you specify an address, the read starts at that address. If you specify a symbol, the read starts at the address of that symbol. You can also enter an expression using a plus sign (+) or a minus sign (-). For example, you could enter cat + 100 and the read would start at 256 bytes passed the address of cat.
 - Length of read (in above units).

Figure 11-27 on page 11-39 shows an example of Read Adapter Memory output. This example was obtained by specifying the following values on the dialog screen:

Unit to read by (word, short, byte): **word**

Address or symbol to start read: **0**

Length of read (in above units): **48**

```

00000000: 06700003 000048A4 00004E0F 00002FE8 .p....H...N.../.
00000010: 2FF7DC80 00000000 00000000 0B000000 /.....
00000020: 0000283A 00000000 D00F22A8 0000D0B0 ..(:....."....
00000030: 00224000 D00F22A8 DEADBEEF DEADBEEF ."@...".....
00000040: DEADBEEF 00000000 00000000 01000000 .....
00000050: 30000000 40000000 200006A4 30000000 0...@... ..0...
00000060: 00000106 00000000 00000000 00000000 .....
00000070: 00000000 00000000 00000000 00000000 .....
00000080: 00000000 00000000 00000000 00000000 .....
00000090: 00000000 00000000 00000000 E01E0000 .....
000000A0: 40000707 40001A9A 40000666 007FFFFF @...@...@..f....
000000B0: 007FFFFF 007FFFFF 007FFFFF 007FFFFF .....

```

Figure 11-27. Example of Read Adapter Memory Output

View Adapter Registers

To view the adapter registers using the System Manager:

1. Log in using a controlling userid. See “Logging In to an IBM 6611” on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use Adapter Debug Facility** on the next menu.
4. Select **View Adapter Registers** on the next menu.
5. Select an adapter from the selector screen. See Table 11-1 on page 11-37 for an explanation of the adapter name.

Figure 11-28 shows an example of View Adapter Registers output.

```

TCTL = 26aa3cH  ACTL = 3H  PCTL = 267040H

***GLOBAL REGISTERS***
G0 = deadbeeFH  G1 = 2941H  G2 = 0H  G3 = 28aea0H
G4 = 2f0014H  G5 = 3FH  G6 = 26a614H  G7 = 18000H
G8 = 0H  G9 = 156H  G10 = a18H  G11 = 1000H
G12 = 0H  G13 = 2f0000H  G14 = 20H  FP = 26de50H

***LOCAL REGISTERS***
PFP = 267040H  SP = 3H  RIP = 3f000001H  R3 = 26aa3cH
R4 = 20000H  R5 = 0H  R6 = 0H  R7 = 0H
R8 = 0H  R9 = 0H  R10 = 0H  R11 = 0H
R12 = 0H  R13 = 0H  R14 = 0H  R15 = 0H

```

Figure 11-28. Example of View Adapter Registers Output

Start Adapter Line Trace

The adapter line trace can be used to determine what data was sent and received by the IBM 6611 through the peer-capable adapters. Only one adapter line trace can be running at a time. The line trace record size is 1 K.

Note: Running this trace may degrade system performance.

```

record 1
00000000: 00000000 00000000 00000000 00000000 .....
00000010: A0000000 FFFFA004 FFFFFFFF 8068FFFF .....h..
00000020: 0A003781 FFFFFFFF FFFFFFFF 01003000 ..7.....0.
00000030: 93190000 FFFFFFFF 5304FFFF 93190000 .....S.....
00000040: 135A0008 53045D21 00000200 02008085 .Z..S."!.....
00000050: 00000300 01009219 00000200 00000000 .....
00000060: 00000000 00000000 00000000 00000000 .....
00000070: 00000000 00000000 00000000 80850000 .....
00000080: 00000000 51040100 00000200 00000000 .....Q.....
00000090: 00000000 00000000 00000000 00000000 .....
000000A0: 00000000 00000000 00000000 00000000 .....
000000B0: 00000000 00000000 00000000 00000000 .....
000000C0: 00000000 00000000 00000000 00000000 .....
000000D0: 00000000 00000000 00000000 00000000 .....
000000E0: 00000000 00000000 00000000 00000000 .....
000000F0: 00000000 00000000 00000000 00000000 .....
00000100: 00000000 00000000 00000000 00000000 .....
00000110: 00000000 00000000 00000000 00000000 .....
00000120: 00000000 00000000 00000000 00000000 .....
00000130: 00000000 00000000 00000000 00000000 .....
00000140: 00000000 00000000 00000000 00000000 .....
00000150: 00000000 00000000 00000000 00000000 .....
00000160: 00000000 00000000 00000000 00000000 .....
00000170: 00000000 00000000 00000000 00000000 .....
00000180: 00000000 00000000 00000000 00000000 .....
00000190: 00000000 00000000 00000000 00000000 .....
000001A0: 00000000 00000000 00000000 00000000 .....
000001B0: 00000000 00000000 00000000 00000000 .....
000001C0: 00000000 00000000 00000000 00000000 .....
000001D0: 00000000 00000000 00000000 00000000 .....
000001E0: 00000000 00000000 00000000 00000000 .....
000001F0: 00000000 00000000 00000000 00000000 .....
00000200: 00000000 00000000 00000000 00000000 .....
00000210: 00000000 00000000 00000000 00000000 .....
00000220: 00000000 00000000 00000000 00000000 .....
00000230: 00000000 00000000 00000000 00000000 .....
00000240: 00000000 00000000 00000000 00000000 .....
00000250: 00000000 00000000 00000000 00000000 .....
00000260: 00000000 00000000 00000000 00000000 .....
00000270: 00000000 00000000 00000000 00000000 .....
00000280: 00000000 00000000 00000000 00000000 .....
00000290: 00000000 00000000 00000000 00000000 .....
000002A0: 00000000 00000000 00000000 00000000 .....
000002B0: 00000000 00000000 00000000 00000000 .....
000002C0: 00000000 00000000 00000000 00000000 .....
000002D0: 00000000 00000000 00000000 00000000 .....
000002E0: 00000000 00000000 00000000 00000000 .....
000002F0: 00000000 00000000 00000000 00000000 .....
00000300: 00000000 00000000 00000000 00000000 .....
00000310: 00000000 00000000 00000000 00000000 .....
00000320: 00000000 00000000 00000000 00000000 .....
00000330: 00000000 00000000 00000000 00000000 .....
00000340: 00000000 00000000 00000000 00000000 .....
00000350: 00000000 00000000 00000000 00000000 .....
00000360: 00000000 00000000 00000000 00000000 .....
00000370: 00000000 00000000 00000000 00000000 .....
00000380: 00000000 00000000 00000000 00000000 .....
00000390: 00000000 00000000 00000000 00000000 .....
000003A0: 00000000 00000000 00000000 00000000 .....
000003B0: 00000000 00000000 00000000 00000000 .....
000003C0: 00000000 00000000 00000000 00000000 .....
000003D0: 00000000 00000000 00000000 00000000 .....
000003E0: 00000000 00000000 00000000 00000000 .....
000003F0: 00000000 00000000 00000000 00000000 .....

```

Figure 11-29. Sample Adapter Line Trace Output - Record 1

To start a line trace on an adapter using the System Manager:

1. Log in using a controlling userid. See “Logging In to an IBM 6611” on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use Adapter Debug Facility** on the next menu.
4. Select **Start Adapter Line Trace** on the next menu.

5. Select an adapter from the selector screen. See Table 11-1 on page 11-37 for an explanation of the adapter name.

Figure 11-30 shows an example of the message you receive when you start an adapter line trace.

The line trace has been started. Go to Stop Adapter Line Trace when you want to stop it. When the line trace is stopped, it will be placed in pd_trtya0.linetrace.

Figure 11-30. Example of Start Adapter Line Trace Message

6. On the dialog screen, enter the number of packets to capture in the trace. The adapter trace stops when the specified number of packets are collected.

Dump Adapter Memory

To dump the memory of an adapter using the System Manager:

1. Log in using a controlling userid. See “Logging In to an IBM 6611” on page 9-23 for information about controlling userids.
2. Select **Problem Determination Facilities** from the main menu.
3. Select **Use Adapter Debug Facility** on the next menu.
4. Select **Dump Adapter Memory** on the next menu.
5. Select an adapter from the selector screen. See Table 11-1 on page 11-37 for an explanation of the adapter name.

The adapter dump is placed in the transfer directory.

Figure 11-31 shows an example of the message you receive when you issue an adapter dump. See Figure 11-32 on page 11-42 for a sample of the dump output.

The dump for adapter, trtya0, has been completed.
The adapter dump output is located in the
transfer directory in the following files:
pd_trtya0.dram
pd_trtya0.prom
pd_trtya0.regs
pd_trtya0.sram.

Figure 11-31. Example of Dump Adapter Memory Message

View Adapter Debug Data in Transfer Directory

To view the adapter debug data using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use Adapter Debug Facility** on the next menu.
3. Select **View Adapter Debug Data in Transfer Directory** on the next menu.
4. Select an adapter debug output file from the list of adapter debug files in the transfer directory shown on the selector screen.

Figure 11-32 on page 11-42 shows an example of an adapter dump being viewed with this menu item.

00000000:	00000000	00000140	00000000	00000B60	@.....
00000010:	FFFFF360	00000000	00000000	FFFFFFF	
00000020:	32393931	36303130	38323730	20203332	299160108270 32
00000030:	31313636	63694D20	6F636F72	28206564	1166ciM ocor(ed
00000040:	43202943	7279706F	74686769	4D424920	C)CryptohgiMBI
00000050:	726F4320	31202E70	2C303939	39393120	roC 1 .p,099991
00000060:	20202E31	206C6C41	68676972	72207374	.1 l1Ahgirr st
00000070:	72657365	2E646576	00000710	304000FB	rese.dev....0@..
00000080:	00000000	00000000	00000000	00FC00FB	
00000090:	00000000	00000000	00000710	00FC00A3	
000000A0:	00000000	00000000	00000710	00FC00A3	
000000B0:	00000000	00000000	00000000	00000000	
000000C0:	00000000	00000000	00000000	00000000	
000000D0:	00000000	00000000	00000000	00000000	
000000E0:	00000000	00000000	00000000	00000000	
000000F0:	00000000	00000000	00000000	00000000	
00000100:	00000000	00000000	00000000	00000000	
00000110:	00000000	00000000	00000000	00000000	
00000120:	00000000	00000000	00000000	00000000	
00000130:	00000000	00000000	00000000	00000000	
00000140:	00000000	0000000C	00000000	00000000	
00000150:	00000000	000001F0	00070000	00000000	
00000160:	000001FF	0000027F	00000600	00000000	

Figure 11-32. Example of View Adapter Debug Data in Transfer Directory Output

Use Source Route Bridging Debug Facility

When you are debugging a bridge that is configured for source route bridging, there are several tasks that can examine the problems occurring on the bridge.

Figure 11-33 on page 11-43 shows the menu screen for Use Source Route Bridging Debug Facility.

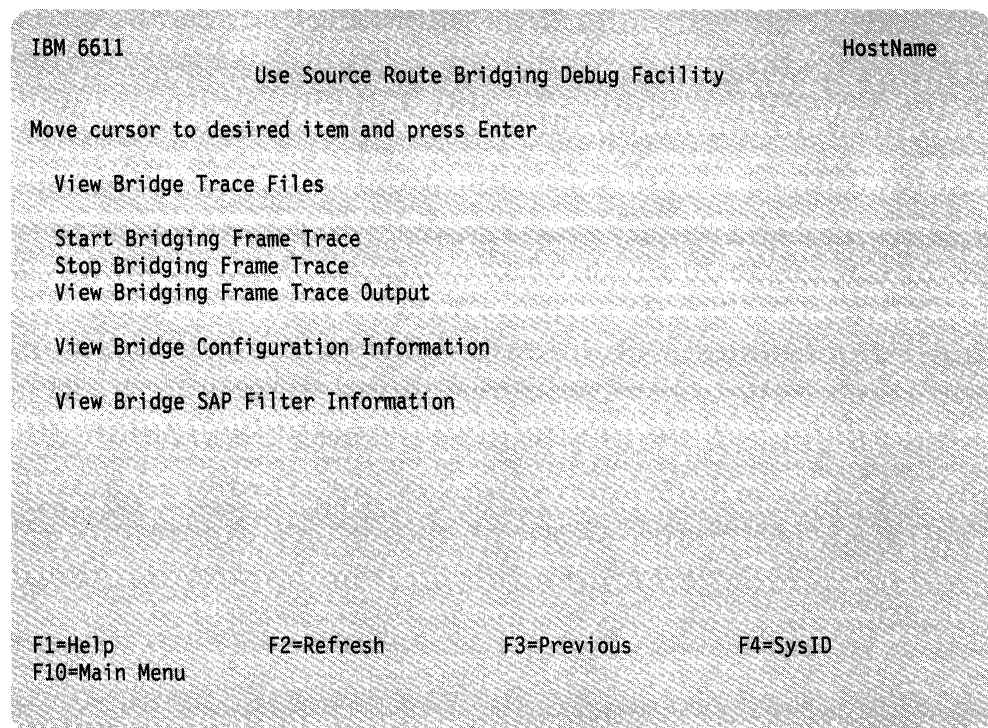


Figure 11-33. Use Source Route Bridging Debug Facility Menu

This facility is used with these peer-capable adapters:

- Token-Ring Network 16/4 Adapter
- EIA 422/449 Serial Adapter
- V.35/V.36 Serial Adapter.

Table 11-2 explains the methodology for the interface names for these adapters. These interface names are used with most of the commands in the Bridging Debug Facility.

Table 11-2. Adapter Interface Name Table

Adapter Name	Interface Name
Token-Ring Network 16/4 Adapter	tk#
EIA 422/449 Serial Adapter	to?
V.35/V.36 Serial Adapter	to?

The number sign, (#), can be a number from 0 - 6. The question mark, (?), can be a number from 0 - 13. The number corresponds to the order of that particular interface type as it is located in the IBM 6611. For example, to0 corresponds to the first port of the first 2-port serial adapter and tk1 corresponds to the second token-ring adapter.

This Bridging Debug Facility is not used in normal operation of the IBM 6611. It is used by service representatives to troubleshoot bridging problems with the peer-capable adapter software.

See these pages for more information about the individual menu items:

View Bridge Trace Files	11-44
Start Bridging Frame Trace	11-44
Stop Bridging Frame Trace	11-45
View Bridging Frame Trace Output	11-45
View Bridge Configuration Information	11-46
View Bridge SAP Filter Information	11-47

View Bridge Trace Files

To view the bridge trace files using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use Source Route Bridging Debug Facility** on the next menu.
3. Select **View Bridge Trace Files** on the next menu.
4. Select the type of bridge trace file that you want to view. The choices are as follows:
 - LAN bridge protocol trace
 - pd_bnpmanp
 - pd_bnbmast
 - pd_bnbrifh
 - Spanning tree trace
 - pd_sptmain

Figure 11-34 shows an example of the pd_sptmain file.

```

Wed Jul 15 10:45:59 1992 : Waiting for protocfgd SIGHUP signal, port number= 0, errno= 0.
Wed Jul 15 10:50:25 1992 : Waiting for protocfgd SIGHUP signal, port number= 0, errno= 0.
Wed Jul 15 10:51:17 1992 : Got protocfgd SIGHUP signal, port number= 0, errno= 0.
Wed Jul 15 10:51:18 1992 : Spanning tree configuration table ...
    ENABLE_BRIDGING:1, BRDG_NUMBER:1, DES_RNG_NUM:0001, BRDG_PRI:8000,
    HELLO:0200, FRWD_DELAY:0f00, MAX_AGE:1400,
    NUM_LOG_PORTS:15, NUM_PHY_PORTS:3, NUM_BN_PORTS:2,
Logical port 2 : IFNAME:to0, SLOT#:1, PORT#:0,
                  : ADAPT_TYPE:3, SERIAL_PROTO:2, PHYS_NUMBER:1,
                  : USE_UNIV_ADDR:0, MAC_ADDR_CAN:000000000000, RING_SPEED:0,
                  : PERF_CNT_THRESH:10, LNK_ERROR_THRESH:0, AUTO_REBOOT:1,
                  : MEM_DUMP_DRV:0, EVNT_LOG_DRV:0, LRG_FRM_SIZE:2, LN_SPEED:19200,
                  : RPS:1, REM:1, CRS:1,
                  : LNK_PSWD0_PRESENT:0, PSWD0:
  
```

Figure 11-34. Example of Use Source Route Bridging Debug Facility Output

Start Bridging Frame Trace

This task can be used to capture a few frames to see what bridging is doing with them. The capture buffer is limited to 32 frames. If you set the number of frames to capture to 32, the trace will capture 32 frames, and then stop capturing them. The buffer is saved. If you set the number of frames to capture to 800, the buffer will hold the last 32 frames. The bridge frame trace stops capturing frames after 800 frames have been captured.

To start a bridging frame trace:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use Source Route Bridging Debug Facility** on the next menu.
3. Select **Start Bridging Frame Trace** on the next menu.
4. Select an adapter interface name from the selector screen. See Table 11-2 on page 11-43 for an explanation of the interface name.
5. On the dialog screen, enter the number of frames to capture. Any value between 1 and 800 is acceptable. Press **Tab** to select the direction of the frames to trace. The choices are **transmit, receive, or both**.

Figure 11-35 shows an example of the message you receive when you start the bridge trace.

The trace has been started. Be sure to stop the trace before attempting to view it.

Figure 11-35. Example of Start Bridging Frame Trace Message

Stop Bridging Frame Trace

To stop a bridging frame trace using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use Source Route Bridging Debug Facility** on the next menu.
3. Select **Stop Bridging Frame Trace** on the next menu.
4. Select an adapter interface name from the selector screen. See Table 11-2 on page 11-43 for an explanation of the interface name.
5. On the dialog screen, press **Tab** to select the direction of the frames in the trace. The choices are **transmit, receive, or both**.

Figure 11-36 shows an example of the message you receive when you stop the bridging frame trace.

The trace is stopped. It can be viewed using View Bridging Frame Trace Output.

Figure 11-36. Example of Stop Bridging Frame Trace Message

View Bridging Frame Trace Output

To view a bridging frame trace output using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use Source Route Bridging Debug Facility** on the next menu.
3. Select **View Bridging Frame Trace Output** on the next menu.
4. Select the destination for the bridge frame trace output (**screen** or **transfer_directory**) from the selector screen.
5. Select an adapter interface name from the selector screen. See Table 11-2 on page 11-43 for an explanation of the interface name.

6. On the dialog screen, press **Tab** to select the direction of the frames in the trace. The choices are **transmit**, **receive**, or **both**.

Figure 11-37 shows an example of the output from the bridging frame trace.

SRB Captured TX frames:

```
-----
Sequence #:      0
Length:         78
Frame Type:    0x01
Action:        0x00

00 03 00 0A 00 00 00 10 FF FF 18 40 FF FF FF FF FF FF C0 00 66 11 00 60
84 30 00 11 AA AA 03 00 00 00 08 00 45 00 00 34 7B DE 00 00 01 11 08 4F
00 00 00 00 00 00

-----
Sequence #:      1
Length:         78
Frame Type:    0x01
Action:        0x00

00 03 00 0A 00 00 00 10 FF FF 18 40 FF FF FF FF FF FF C0 00 66 11 00 60
84 30 00 11 AA AA 03 00 00 00 08 00 45 00 00 34 7B DE 00 00 01 11 08 4F
00 00 00 00 00 00

-----
Sequence #:      2
Length:         76
Frame Type:    0x01
Action:        0x00

00 03 00 0A 00 00 00 10 00 00 18 40 C0 00 20 00 00 00 C0 00 66 11 00 60
C4 30 00 11 AA AA 03 00 00 00 60 03 1B 00 0B 02 00 00 AA 00 04 00 09 C7
00 00 00 00 00 00
-----
```

SRB Captured RX frames:

Figure 11-37. Example of View Bridging Frame Trace Output

View Bridge Configuration Information

This task allows you to determine whether a bridge is active on a particular adapter. The bridge table is displayed for the selected adapter. If the output contains a list of rings and other information, a bridge is configured on that adapter. If zeros are returned as the output, a bridge has not been configured on that adapter.

To view bridge configuration information using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use Source Route Bridging Debug Facility** on the next menu.
3. Select **View Bridge Configuration Information** on the next menu.
4. Select the destination for the bridge configuration information output (**screen** or **transfer_directory**) from the selector screen.

5. Select an adapter interface name from the selector screen. See Table 11-2 on page 11-43 for an explanation of the interface name.

Figure 11-38 shows an example of the output you receive when you view bridge configuration information.

SRB Table MIB Data								
Ring	Adap	Port	MaxLen	MaxFld	Stat	MaxHop	Bridge	DesRing
000	0f	00	2052	20	23	7	1	ffffff
001	00	00	2052	20	47	7	1	ffffff
002	01	00	2052	20	53	7	1	001
003	01	01	2052	20	53	7	1	001

Figure 11-38. Example of View Bridge Configuration Information Message

View Bridge SAP Filter Information

After determining that a bridge is configured on an adapter, this task shows the status of the SAP filters. All the filters can be viewed using this task. The SAP filter is important because it tells you which SAPs the bridge is routing and which SAPs the bridge is bridging. It also determines which SAPs are using data link switching.

To view bridge SAP filter information using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use Source Route Bridging Debug Facility** on the next menu.
3. Select **View Bridge SAP Filter Information** on the next menu.
4. Select the destination for the bridge configuration information output (**screen** or **transfer_directory**) from the selector screen.
5. Select an adapter interface name from the selector screen. See Table 11-2 on page 11-43 for an explanation of the interface name.

Figure 11-39 shows an example of the output you receive when you view bridge SAP filter information.

```

SRB SAP MIB Data:
  SAPInBCType:          01  SAPOutBCType:          01
  NumSNAPInTableEntries: 0  NumSNAPOutTableEntries: 0
  SNAPInInclude:        00  SNAPOutInclude:        00
  SAPInNotForwarded:    0  SAPOutNotForwarded:    0
  SNAPInNotForwarded:    0  SNAPOutNotForwarded:    0

  SAPTableIn:  fffffffffffffffffffffdffffffffffff
  SAPTableOut: fffffffffffffffffffffdffffffffffff
  SystemSAPTable: 00000000000000000000000000000000

```

Incoming SNAP Table 0 Entries:

Outgoing SNAP Table 0 Entries:

Figure 11-39. Example of View Bridge SAP Filter Information Output

Use DECnet Debug Facility

The DECnet Debug facility provides helpful information for debugging problems with the DECnet protocol. You can view the DECnet routing data structures, run the DECnet trace and view the DECnet trace output.

Figure 11-40 shows the menu screen for Use DECnet Debug Facility.

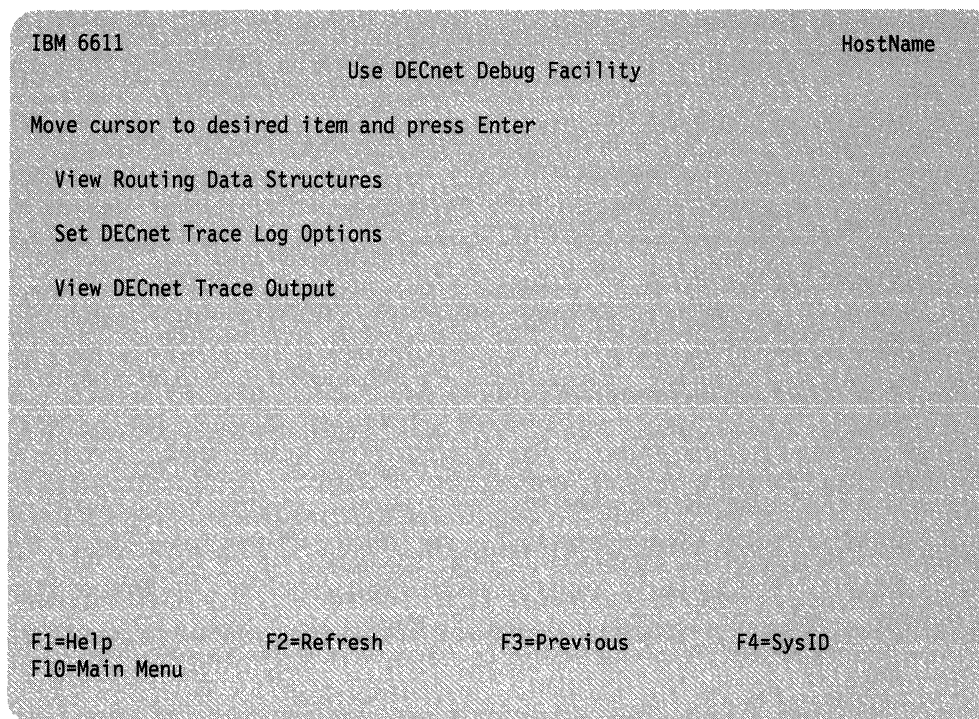


Figure 11-40. Use DECnet Debug Facility Menu

This DECnet Debug Facility is not used in normal operation of the IBM 6611. It is used by service representatives to troubleshoot DECnet protocol problems.

See these pages for more information about the individual menu items:

View Routing Data Structures	11-48
Set DECnet Trace Output	11-50
View DECnet Trace Output	11-52

View Routing Data Structures

The DECnet Debug Facility allows you to view the DECnet routing data structures. You can select to view the whole data structure (or as much of the data structure as can be viewed at once), starting with the first entry, or to view only a specified number of entries in the data structure starting with a specified entry.

To view the DECnet routing data structures using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use DECnet Debug Facility** on the next menu.
3. Select **View Routing Data Structures** on the next menu.
4. Select the data structure that you want to view from the selector screen. The choices are as follows:

- DECnet hop matrix
 - DECnet cost matrix
 - DECnet minimum hop vector
 - DECnet minimum cost vector
 - DECnet area hop matrix
 - DECnet area cost matrix
 - DECnet area minimum hop vector
 - DECnet area minimum cost vector
 - DECnet reach vector
 - DECnet area reach vector
 - DECnet output adjacency vector
 - DECnet area output adjacency vector
 - DECnet adjacency vector
 - DECnet circuit vector
 - DECnet executor data structure.
5. Select the destination for the data structure output (**screen** or **transfer_directory**) from the next selector screen.
6. On the dialog screen for each of the data structures except for the executor data structure, specify the starting entry to display. The default is to start with the first entry. The maximum starting entry for each data structure is as follows:
- 1023 — hop matrix
 - 1023 — cost matrix
 - 1023 — minimum hop vector
 - 1023 — minimum cost vector
 - 63 — area hop matrix
 - 63 — area cost matrix
 - 63 — area minimum hop vector
 - 63 — area minimum cost vector
 - 1023 — reach vector
 - 63 — area reach vector
 - 1023 — output adjacency vector
 - 63 — area output adjacency vector
 - 1023 — adjacency vector
 - 14 — circuit vector.

Specify the number of entries to display. The default is all the entries, except for the hop and cost matrices and the adjacency vector. For each of these the maximum you can display is 400 entries. The maximum number of entries for each data structure is as follows:

- 400 — hop matrix
- 400 — cost matrix
- 1023 — minimum hop vector
- 1023 — minimum cost vector
- 63 — area hop matrix
- 63 — area cost matrix
- 63 — area minimum hop vector
- 63 — area minimum cost vector
- 1023 — reach vector
- 63 — area reach vector
- 1023 — output adjacency vector
- 63 — area output adjacency vector
- 400 — adjacency vector
- 14 — circuit vector.

Figure 11-41 shows an example of a circuit vector entry. Figure 11-42 shows an example of the executor data structure.

```
CIR(1)
state = ON
Circuit Name = tk0          Circuit-Type = TOKEN
Cost = 3                   Hello Time = 15
Router_Priority = 64       Designated Router_Priority = 64
Max Numof Routers = 32    Numof Routers Sofar = 0
LineDeviceName = trtya0   LineIndex/If_index = 3
LineMaxBlock/DataLinkBuffSize = 1498
```

Figure 11-41. Example of Circuit Vector Entry

```
Executor Address = 48.1000
Executor Area = 48.774202368 Node = 1000.808596278
Node Type = Level 2-Router
State = ON
Maximum Visits = 63
Maximum Cost = 1022
Maximum Hops = 30
Area Maximum Cost = 1022
Area Maximum Hops = 30
Maximum Node Address = 1023
Maximum AreaNode Address = 63
Maximum Broadcast Router Adjacencies = 32
Maximum Broadcast End-Node Adjacencies = 1022
Routing Buffer Size = 1498
```

Figure 11-42. Example of Executor Data Structure

Set DECnet Trace Output

The DECnet trace is always running. The trace data can be logged with some system trace data or by itself.

The trace debug level specifies the trace points that are activated. The debug levels range from 0 to 15. If a debug level of '0' is chosen, only error conditions are traced. If a debug level of '15' is chosen, all trace points are recorded.

The trace mask is a 32-bit number that is specified in hexadecimal. Each bit represents a specific action that can occur and for which a trace entry can be recorded. If the bit is on, a trace entry is recorded when the specific action occurs, if the action has a debug level less than or equal to the current debug level. The trace time stamp mask is a 32-bit hexadecimal digit representing the same actions. If the bit is on, a time stamp is recorded whenever a trace entry is recorded for the specific action. Any combination of bits may be on. The individual bits in the trace mask have the following meanings:

• When any packet is received	X'00000001'
• When a Level 1/2 packet is received	X'00000002'
• When processing a Level 1 packet	X'00000004'
• When processing a Level 2 packet	X'00000008'
•	
• When the routing timer for broadcast circuit expires	X'00000010'
• When sending a route update	X'00000020'
• When sending a short route update quickly	X'00000040'
• When sending a Level 1/2 route message	X'00000080'
•	
• When locating an adjacency	X'00000100'
• When processing an R/S list in a received router Hello	X'00000200'
• When formatting a router Hello packet	X'00000400'
• When receiving a router/end Hello packet	X'00000800'
•	
• When processing a configuration change	X'00001000'
• When processing a circuit state change	X'00002000'
• When processing a circuit cost change	X'00004000'
• When processing a change in maximum values	X'00008000'
•	
• When a maximum value is exceeded	X'00010000'
• When in Phase IV prime specific processing	X'00020000'
• When a packet with errors is received	X'00040000'
• When in Ki-Research processing	X'00080000'
•	
• When in routes and area routes processing	X'00100000'
• When in route change processing	X'00200000'
• When in nearest Level-2 router processing	X'00400000'
• When in attached flag related processing	X'00800000'
•	
• When in adjacency state change related processing	X'01000000'
• When in designated router related processing	X'02000000'
• When processing the routing timer	X'04000000'
• When processing events marked as interesting	X'08000000'
•	
• When processing the express queue	X'10000000'
• When in routing buffer-size related processing	X'20000000'
• When in DNArouted-Scram interface processing	X'40000000'
• When processing network inconsistencies	X'80000000'

The DECnet Debug Facility allows you to set the DECnet trace options that include:

- specifying the destination of the trace output
- setting the trace debug level
- setting the trace mask
- setting the trace time stamps to record.

To set the DECnet trace options using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use DECnet Debug Facility** on the next menu.
3. Select **Set DECnet Trace Output** on the next menu.
4. On the dialog screen use **Tab** to select the destination of the trace output. Select **system** to send the trace output to the System Monitor Trace log or **DECnet** to send the trace output to the DECnet Trace log. If you change the

location of the trace output the change does not take effect until DECnet is restarted.

Type the debug level, any number from 0 to 15. If this field is not specified, the debug level is unchanged from its previous setting. The initial setting of the debug level is '0'.

Type the trace mask. Any hex digit from X'00000000' to X'FFFFFFFF' is valid. If this field is not specified, the trace mask is unchanged from its previous setting. The initial setting of the trace mask is X'00000000'.

Type the trace time stamp mask. Any hex digit from X'00000000' to X'FFFFFFFF' is valid. If this field is not specified, the trace time stamp mask is unchanged from its previous setting. The initial setting of the trace time stamp mask is X'00000000'.

View DECnet Trace Output

The DECnet trace is always running. The trace output is either logged with some system trace data or by itself. You can view the DECnet trace output.

To view the DECnet trace output using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Use DECnet Debug Facility** on the next menu.
3. Select **View DECnet Trace Output** on the next menu.
4. On the selector screen select the source of the trace output, specify **system** to view the trace output in the System Monitor Trace log or **DECnet** to view the trace output in the DECnet Trace

The command status screen displays the trace output.

Figure 11-43 shows an example of DECnet trace output from the DECnet trace log.

```
format_rt_hello: add node name to ext
format_rt_hello: sending rt hello to ALL ENDNODES
format_rt_hello: add node name to ext
Mon Oct 26 01:25:48 1992
  bctlmr_handler: for adj 1
bctlmr_handler: for adj 1
routes s 0 e 1023
Mon Oct 26 01:25:48 1992
  rtupdate: level 1 adj 1 resume 0
rtupdate() level 1 adj 1 resume 0
Mon Oct 26 01:25:48 1992
  send_rtmsg1: try on cir 1 #node 1024 start 512
Mon Oct 26 01:25:48 1992
  send_rtmsg1: try on cir 1 #node 282 start 230
aroutes s 1 e 63
routes s 0 e 0
```

Figure 11-43. Example of DECnet Trace Output

Copy Error Log or Trace Log to Transfer Directory

If the error report or the system trace report that you want to generate is too large to be contained in the transfer directory, it may be necessary to run the reports in another IBM 6611. You can transfer the error log or the trace log to another node to be used to produce a report at that location. In this scenario, the service representative can request that you send in the error or trace log instead of the report.

To copy an error log or trace log to the transfer directory using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Copy Error Log or Trace Log to Transfer Directory** on the next menu.
3. Select a log to transfer (**error** or **trace**) from the selector screen.

Figure 11-44 shows an example of the message you receive when you copy the error log to the transfer directory.

Copied error log file to pd_error.log in transfer directory

Figure 11-44. Example of Copy Error Log or Trace Log to Transfer Directory Output

Export Problem Determination Output

To export problem determination output using the System Manager:

1. Select **Problem Determination Facilities** from the main menu.
2. Select **Export Problem Determination Output** on the next menu.
3. Select an export method from the selector screen.
 - FTP
 - Modem
 - DOS diskette
 - UNIX diskette.
4. With each of these file transfer methods, a selector screen appears requesting the name of the file to be transferred. Select the name of the problem determination output file.
 - Transferring files with FTP requires you to give the host name and a userid at the destination node on the dialog screen. You are prompted for the password for the userid.
 - Transferring files to a DOS diskette requires you to give the name of the file on the DOS diskette.
 - Transferring files to a UNIX diskette requires you to specify whether to *append* the file to the end of the diskette or to place it as the only file on the diskette, *create*.

Figure 11-45 shows an example of the messages you receive while exporting an error report to a workstation that is modem attached.

```
Return to your local machine and begin file transmission.
The system is ready to send file pd_error.report.
      Use Ctrl+X to stop xmodem.
```

Figure 11-45. Example of Export Problem Determination Output Using Modem

Using the IBM 6611 Performance and Statistics Facilities

The IBM 6611 logs various types of performance and statistics data. Data can be gathered about the performance of many of the components in the IBM 6611, including:

- Main operating system
- Running user processes
- Installed peer-capable adapters
 - Token-Ring Network 16/4 Adapter
 - Ethernet Adapter
 - EIA 422/449 Serial Adapter
 - V.35/V.36 Serial Adapter
- Configured protocols
- Fixed disks
- Network, as viewed from both the peer-capable adapters and the main system.

The SNMP MIB variables can also be viewed. Refer to the *IBM 6611 Network Processor Network Management Reference* for more information about MIBs.

The performance data generated about most of these components is designed to be used for problem determination by IBM service personnel. This book does not attempt to explain or interpret the details of the performance output. If IBM service personnel are not given remote access to this IBM 6611 for problem determination, you could be asked to retrieve some of this performance data.

To gather performance data, select **Performance and Statistics** from the System Manager main menu, and the menu in Figure 11-46 on page 11-55 is displayed.

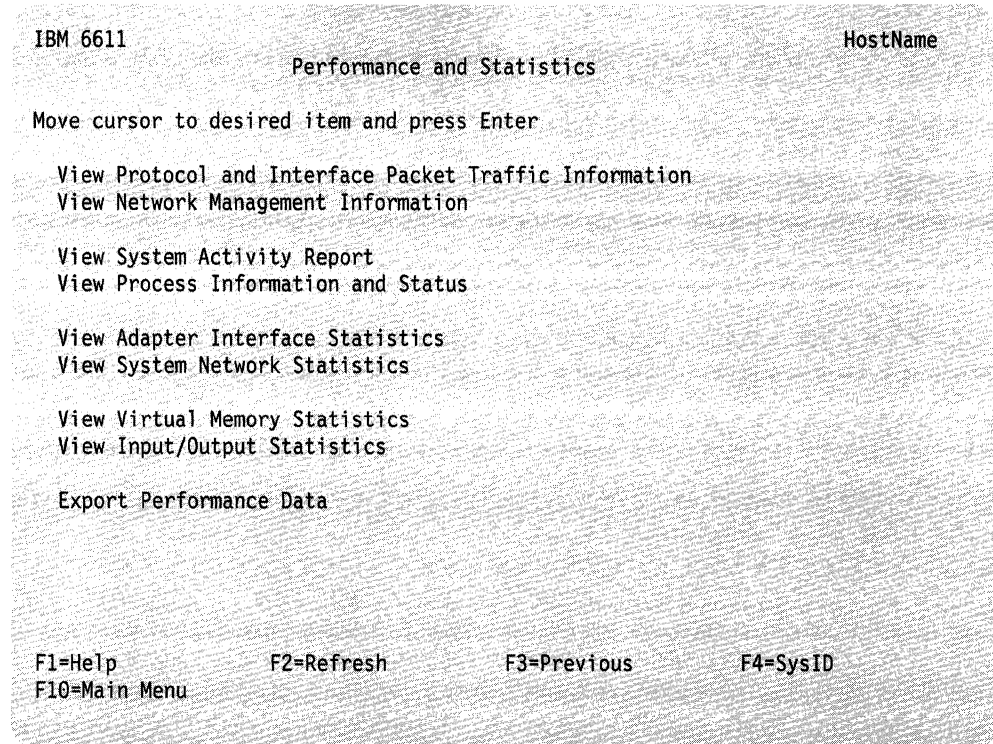


Figure 11-46. Performance and Statistics Menu

See these pages for more information about the individual menu items:

View Protocol and Interface Packet Traffic Information	11-55
View Network Management Information	11-57
View System Activity Report	11-59
View Process Information and Status	11-61
View Adapter Interface Statistics	11-69
View System Network Statistics	11-75
View Virtual Memory Statistics	11-87
View Input/Output Statistics	11-88
Export Performance Data	11-89

These tasks can be invoked using command primitives. See Chapter 8 for information about the command primitives.

View Protocol and Interface Packet Traffic Information

There is a single screen adapter interface and protocol monitor that is useful for checking to see if the adapters and protocols are actively passing traffic. It reports the number of packets sent and received for the adapter or protocol. The reporting is done at the adapter interface level. The packet traffic screen is continually updated, until you chose to stop it.

This screen also shows the state of the adapters and protocols. If a protocol is listed as **up**, the protocol is enabled and the process is running. If the protocol is listed as **down**, either the protocol is not enabled or, if it is enabled, the process is stopped. Only the adapters that are present are listed. If an adapter is listed as **down**, it is present, but not configured. If an adapter is listed as **up**, it is present and configured.

To view protocol and interface packet traffic information using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View Protocol and Interface Packet Traffic Information** from the next menu.
3. Enter the number of seconds between screen updates on the dialog screen.
Enter a number between 5 and 10. Only values greater than or equal to 5 are valid.
4. Press **Ctrl + C** to end this command.

Figure 11-47 shows an example of View Protocol and Interface Packet Traffic Information output.

PACKET TRAFFIC INFORMATION FOR PROTOCOLS AND INTERFACES

Protocol	rcv	xmt	Status	Interface	rcv	xmt	Status
ip:	13188	13405	up	lo0:	7014	7014	up
tcp:	3483	3600	up	te0:	179	179	up
udp:	2677	2955	up	te1:	172	172	up
snmp:	1380	1500	up	tk0:	189	171	up
ppp:	0	0	down	te2:	171	171	up
decnet:	0	0	down	to0:	0	0	down
dls:	0	0	down				
FmRI:	0	0	down				
Brdg:	0	0	down				
ipx:	0	0	down				
xns:	0	0	down				
APPN:	0	0	down				
AppTk:	0	0	down				
TBrdg:	0	0	down				
Press Ctrl+C to return to System Manager.							

Figure 11-47. Sample View Protocol and Interface Packet Traffic Information Panel

The interfaces for which packet traffic is being reported are loopback and the peer-capable adapters. See Table 11-3 on page 11-57 for an explanation of the interface name. The number sign (#) can be a number from 0 to 6. The question mark (?) can be a number from 0 to 13. The dollar sign (\$) is either 0 or 1. The number corresponds to the order of that particular interface type as it is located in the IBM 6611. For example, *te0* corresponds to the first Ethernet adapter and *tk1* corresponds to the second Token Ring adapter.

Table 11-3. Interface Name Table

Adapter or Interface	Interface Name
Token-Ring Network 16/4 Adapter	tk#
Ethernet Adapter	te#
EIA 422/449 Serial Adapter	to?
V.35/V.36 Serial Adapter	to?
Loopback	lo\$

View Network Management Information

The SNMP network management data that is gathered for all the adapters and the base operating system can be viewed. The output you receive is based on the MIB variable that you select and the type of request.

To view network management information using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View Network Management Information** from the next menu.
3. Select a MIB module to be viewed from the list in the selector screen.

A management information base (MIB) module is a collection of MIB variables relating to a common management area. The module defines each of the MIB variables, providing their syntax, numeric names, and textual names. The MIB module you select will be used to interpret the MIB variable name you provide in the MIB variable being requested entry field.

MIB modules are provided for standard MIBs as well as many vendor specific MIBs. If you are querying an IBM 6611, select **IBM_6611 Complete MIB**. This is the default.

4. Enter or select values for the dialog items that follow:

Type of request.

The following requests are supported:

dump

Requests the value of the specified MIB variable and all of its objects. This request allows you to query MIB variables without knowledge of each instance present. By specifying the first object in the MIB (in the MIB variable being requested entry field) the dump request will allow you to query the entire MIB.

next

Requests the value of the MIB variable following the specified variable. Like the dump request, the next request makes it possible to query MIB variables without knowledge of the instance qualifiers.

get

Requests the value of the specified MIB variable. You must specify the exact instance (in the MIB variable being requested entry field) of the variable you are querying. For example, if you want to query the sysDescr variable in MIB-II, you must specify sysDescr.0. It is often easier to use a dump request for the entire table and then sort through the resulting data until you find the data for which you are looking.

Press **Tab** to select either **dump**, **next**, or **get**.

MIB variable being requested

There are two methods for specifying the MIB variable to be queried:

- a. If you know the name of the desired MIB variable, type it in the entry field. If you have selected get as the type of request, you will use this method.

The variable is specified in Variable.Instance format.

Variable:

Specifies the name in text format or numeric format of a specific MIB variable as defined in the specified MIB module. If the request is next or dump, the Variable parameter can be a MIB group.

Instance:

Specifies the instance qualifier for the MIB Variable parameter. The Instance parameter is required if the request is get. The Instance parameter is optional, if the request is next or dump.

- b. Press **F4 (Esc + 4)** to get a list of all the MIB variables available for the selected MIB module. A very long list is displayed. The list contains only variable groups without instance qualifiers. Press **Enter** to select the desired MIB variable.

Community name to be used with query

This entry field specifies the community name to be used with the query. Each node supporting SNMP is configured with specific communities from which it will accept SNMP commands. A community is a pairing of a community name and an IP address. You must provide a community name that the node you are querying will accept from the address that is issuing the SNMP command. If this value is not specified, a community name, public, is used.

Name of host to be used with query

This entry field specifies the host name or the IP address of the host to be queried for MIB information. If this field is left blank the MIB information is obtained from this IBM 6611. If you specify a host name, the host name must be mapped to an IP address in this IBM 6611 or be translated to one by a name server. You cannot specify an IP address that is associated with the local end of an EIA 422/449 Serial Adapter or a V.35/V.36 Serial Adapter. In order to obtain MIB information from a remote host, there must be an IP route to that host. The IP address format is *nnn.nnn.nnn.nnn*, where *nnn* can be any decimal number from 1 to 255.

Figure 11-48 on page 11-59 shows an example of View Network Management Information output.

```

ifNumber.0 = 6
ifIndex.1 = 1
ifIndex.2 = 2
ifIndex.3 = 3
ifIndex.4 = 4
ifIndex.5 = 5
ifIndex.6 = 6
ifDescr.1 = "lo0; Software Loopback"
ifDescr.2 = "te0; enty0; IBM 6611 Ethernet Network Interface"
ifDescr.3 = "te1; enty1; IBM 6611 Ethernet Network Interface"
ifDescr.4 = "tk0; trty0; IBM 6611 Token-Ring Network Interface"
ifDescr.5 = "te2; enty2; IBM 6611 Ethernet Network Interface"
ifDescr.6 = "to0; t1ty0; IBM 6611 Serial Network Interface"
ifType.1 = softwareLoopback(24)
ifType.2 = ethernet-csmacd(6)
ifType.3 = ethernet-csmacd(6)
ifType.4 = iso88025-tokenRing(9)
ifType.5 = ethernet-csmacd(6)
ifType.6 = t1-carrier(18)
ifMtu.1 = 1536
ifMtu.2 = 1500
ifMtu.3 = 1500
ifMtu.4 = 1500
ifMtu.5 = 1500
ifMtu.6 = 1500
ifSpeed.1 = 0
ifSpeed.2 = 10000000
ifSpeed.3 = 10000000
ifSpeed.4 = 4000000
ifSpeed.5 = 10000000
ifSpeed.6 = 0
ifPhysAddress.1 =
ifPhysAddress.2 = 08:00:5a:13:22:4d
ifPhysAddress.3 = 08:00:5a:13:20:29
ifPhysAddress.4 = 08:00:5a:13:00:6a
ifPhysAddress.5 = 08:00:5a:13:22:18
ifPhysAddress.6 =

```

Figure 11-48. Example of View Network Management Information Output

For additional network management information, refer to the *IBM 6611 Network Processor Network Management Reference*.

View System Activity Report

The system activity report gets the contents of selected cumulative activity counters in the operating system. The accounting system, based on the values in the Number and Interval parameters, writes information the specified number of times at the specified intervals in seconds. There are many system activity functions about which to report.

To view the system activity report using the System Manager:

1. Log in using a controlling userid. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.
2. Select **Performance and Statistics** from the main menu.
3. Select **View System Activity Report** from the next menu.

4. Select a report destination (**screen** or **transfer_directory**) from the selector screen.
5. On the dialog screen, specify the entry fields as follows:

Interval length of each system activity sampling

Type an interval length in seconds.

Number of sampling intervals

Type the number of intervals

Press **Tab** to select either **yes** or **no** on the dialog screen to turn on or off each of the following report options:

- Report all activities listed below?
- Use of file access system routines?
- Buffer activity for transfers, accesses, and cache hit ratios?
- System calls?
- System activity?
- Message and semaphore activities?
- Average queue length while occupied, and percentage of time occupied?
- Paging statistics?
- CPU activity?
- Status of text, process, i-node, and file
- Average queue length while occupied, and percentage of time occupied?
- Percentage of time occupied?
- Serial port terminal activity?

Figure 11-49 shows an example of View System Activity Report output.

```

IBM 6611 mprII 2 3 000009133000    04/23/92

17:49:24
CPU Activity
      %usr    %sys    %wio    %idle
        6        9        1       83

17:49:27
CPU Activity
      %usr    %sys    %wio    %idle
        2       15        0       83

CPU Activity
      %usr    %sys    %wio    %idle
Average    4       12        1       83
  
```

Figure 11-49. Example of View System Activity Report Output

View Process Information and Status

The running user processes in the IBM 6611 have various pieces of statistical information that can be viewed. This information can be useful for debugging problems with the user processes or with the performance of the operating system. The process information can be viewed in five different forms to get the full range of statistics.

Figure 11-50 shows the menu screen for View Process Information and Status.

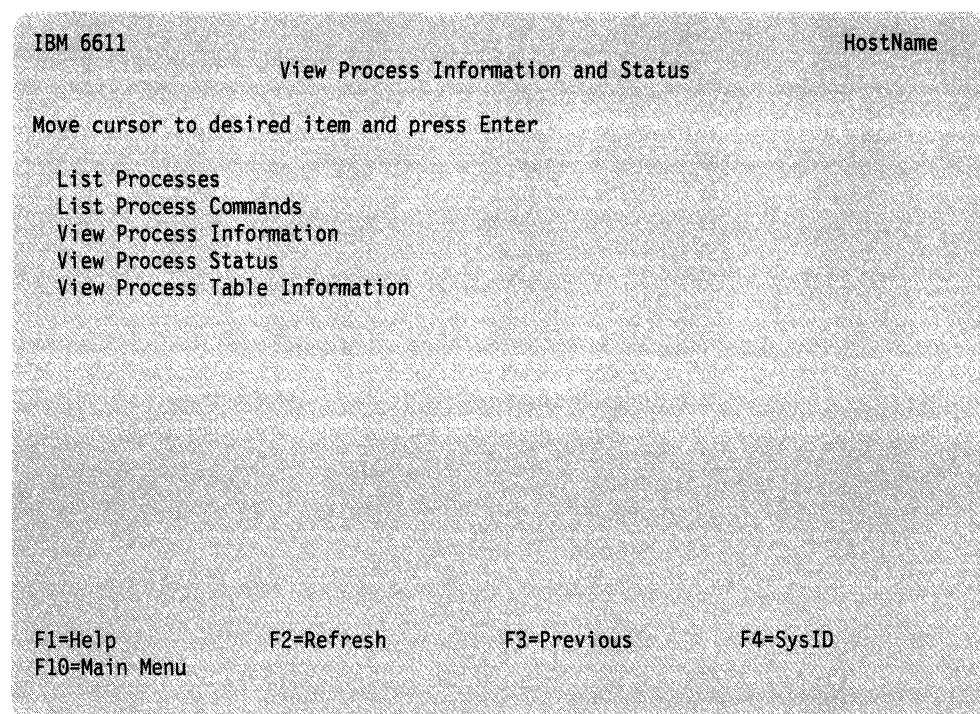


Figure 11-50. View Process Information and Status Menu

See these pages for more information about the individual menu items:

List Processes	11-61
List Process Commands	11-62
View Process Information	11-63
View Process Status	11-65
View Process Table Information	11-67

These tasks can be invoked using command primitives. See “Process Command Primitives” on page 8-68 for information about the command primitives.

List Processes

To list the processes using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View Process Information and Status** on the next menu.
3. Select **List Processes** on the next menu.

The field descriptions for this list are:

PID	The process ID of the process.
USER	The user name of the process owner.
COMMAND	The command name.

Figure 11-51 shows an example of List Processes output.

PID	USER	COMMAND
0	root	swapper
1	root	init
514	1025140	kproc
771	root	kproc
1028	root	kproc
1521	root	snmpd
1577	root	sysmon
2149	root	kproc
2359	root	monproc
2570	root	syncd
2872	root	mondisk
3303	root	cfgdpppd
3340	root	errdemon
3635	root	syslogd
3958	root	kproc
4324	root	ksh
4417	root	cron
4648	root	srcmstr
4890	root	ps
5179	root	rt66cfgd
5436	root	scram
5693	root	t960logd
5950	root	inetd
6629	root	smux.cfgd
6748	root	writesrv
7149	root	lcpd
7261	root	uprintfd
7500	root	qdaemon
7684	root	sleep
8178	root	smux.trapd
8644	root	ksh
8934	root	protocfgd
9203	root	smux.r66d
9460	root	smux.rs960d
9680	root	ksh
9941	root	smitty

Figure 11-51. Example of List Processes Output

List Process Commands

To list the full process commands and parameters using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View Process Information and Status** on the next menu.
3. Select **List Process Commands** on the next menu.

The field descriptions for this list are:

PID The process ID of the process.
COMMAND The full command name and its parameters.

Figure 11-52 shows an example of List Process Commands output.

PID	COMMAND
0	swapper
1	/etc/init
514	kproc
771	kproc
1028	kproc
1521	/usr/sbin/snmpd -c /tmp/snmpd.conf
1577	/etc/sysmon
2149	kproc
2359	/etc/monproc
2570	/etc/syncd 60
2872	/etc/mondisk
3303	/etc/cfgdpppd
3340	/usr/lib/errdemon
3635	/etc/syslogd
3958	kproc
4324	-ksh
4417	/etc/cron
4648	/etc/srcmstr
4890	ps -A -Fpid args cmd
5179	/etc/rt66cfgd
5436	/etc/scram -s
5693	/etc/t960logd
5950	/etc/inetd
6629	/usr/sbin/smux.cfgd
6748	/etc/writesrv
7149	lcpd
7261	/etc/uprintfd
7500	qdaemon
7684	sleep
8178	/usr/sbin/smux.trapd -c /tmp/trapd.config
8644	-ksh
8934	/etc/protocfgd
9203	/usr/sbin/smux.r66d
9460	/usr/sbin/smux.rs960d
9680	-ksh
9941	sysman

Figure 11-52. Example of List Process Commands output

View Process Information

To view process information using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View Process Information and Status** on the next menu.
3. Select **View Process Information** on the next menu.
4. Select a report destination (**screen** or **transfer_directory**) from the selector screen.

The field descriptions for this list are:

F	Flags which are octal and additive and have the following meanings: 01 In core 02 System process 04 Locked in core 10 Waiting for a page default, or forking 20 Being traced by another process 40 Another tracing flag 100 Process has shared text.
S	The state of the process: 0 Nonexistent S Sleeping W Waiting R Running I Intermediate Z Canceled T Stopped K Available system process X Growing
UID	The user ID of the process owner
PID	The process ID of the process
PPID	The process ID of the parent process
C	Processor utilization for scheduling
PRI	The priority of the process; higher numbers mean lower priority.
NI	Nice value; used in calculating priority
ADDR	The segment number of the process stack, if a normal process The address of the preprocess data area, if a system process
SZ	The size in 1024 byte units of the core image of the process
WCHAN	The event for which the process is waiting or sleeping; if blank, the process is running.
TTY	The controlling workstation for the process: - The process is not associated with a workstation. ? The controlling workstation is unknown Number The serial port number minus 1; 0 for S1 and 1 for S2.
	TIME The total execution time for the process
CMD	The command name.

Run List Process Commands from this menu to see the full process command name and parameters. Run List Processes from this menu to see just the process name.

Figure 11-53 shows an example of View Process Information output.

F	S	UID	PID	PPID	C	PRI	NI	ADDR	SZ	WCHAN	TTY	TIME	CMD
b03	S	0	0	0	120	16	--	e07	8		-	0:41	swapper
202803	S	0	1	0	0	60	20	804	228		-	1:23	init
303	R	0	514	0	120	127	--	1008	12		-	1772:31	kproc
303	S	0	771	0	0	39	--	a05	16		-	2:10	kproc
303	S	0	1028	0	0	36	--	140a	16		-	0:00	kproc
260801	S	0	1521	1577	0	60	20	2592	452		-	0:31	snmpd
260801	S	0	1577	1	0	60	20	12e9	2640		-	2:42	sysmon
40a01	S	0	2149	1	0	60	20	c26	16		-	0:00	kproc
240c01	S	0	2359	1577	0	60	20	32f9	96		-	0:49	monproc
240801	S	0	2570	1	0	60	20	2c1	48	595b798	-	0:22	syncd
240c01	S	0	2872	1577	0	60	20	1b0d	96		-	0:26	mondisk
260801	S	0	3303	1577	0	60	20	964	40		-	0:08	cfgdpppd
42801	S	0	3340	1	0	60	20	18cc	212	b838	-	0:52	errdemon
260801	S	0	3635	4648	0	60	20	301	128		-	0:04	syslogd
40201	S	0	3958	1	0	60	20	221	16		-	0:00	kproc
240801	S	0	4324	1	0	60	20	1fef	108		0	0:00	ksh
240801	S	0	4417	1	0	60	20	3f1f	148	587db24	-	0:30	cron
260801	S	0	4648	1	0	60	20	ee7	176		-	0:00	srcmstr
200001	R	0	4896	9941	12	66	20	26f3	96		0	0:00	ps
260801	S	0	5179	1577	0	60	20	2110	320		-	0:17	rt66cfgd
260801	S	0	5436	1577	0	60	20	190c	188		-	10:15	scram
240801	S	0	5693	1577	0	60	20	2512	68	1f64a0	-	0:00	t960logd
260801	S	0	5950	4648	0	60	20	2d16	152		-	0:00	inetd
260801	S	0	6629	1577	0	60	20	1d6e	268		-	0:24	smux.cfgd
240801	S	0	6748	4648	0	60	20	3f3f	88	1f63f0	-	0:00	writesrv
260801	S	0	7149	1	0	60	20	1168	132		-	0:04	lcpd
240801	S	0	7261	1	0	60	20	d46	36	3cad0	-	0:00	uprintfd
240801	S	0	7500	4648	0	60	20	2f37	104		-	0:00	qdaemon
240801	S	0	7684	8644	0	60	20	2a54	48	595b618	-	0:00	sleep
260801	S	0	8178	1577	0	60	20	1f8f	488		-	0:08	smux.trapd
240801	S	0	8644	1	0	60	20	381	100		-	0:12	ksh
260801	S	0	8934	1577	0	60	20	3b7d	144		-	0:02	protocfgd
260801	S	0	9203	1577	0	60	20	2b95	764		-	0:05	smux.r66d
260801	S	0	9460	1577	0	60	20	2f97	708		-	0:12	smux.rs960
200801	S	0	9680	4324	0	60	20	2a34	96		0	0:00	ksh
220001	R	0	9941	9680	20	70	20	2433	1276		0	0:09	smitty

Figure 11-53. Example of View Process Information Output

View Process Status

To view process table information using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View Process Information and Status** on the next menu.
3. Select **View Process Status** on the next menu.
4. Select a report destination (**screen** or **transfer_directory**) from the selector screen.

The field descriptions for this list are:

PID	The process ID of the process
TTY	The controlling workstation for the process: - The process is not associated with a workstation. ? The controlling workstation is unknown Number The serial port number minus 1; 0 for S1 and 1 for S2.
S	The state of the process: 0 Nonexistent S Sleeping W Waiting R Running I Intermediate Z Canceled T Stopped K Available system process X Growing
TIME	The total execution time for the process
PGIN	Number of disk I/Os resulting from references by the process to pages not loaded in core
SIZE	Virtual size of the data section of the process (in 1K byte units)
RSS	Real memory (resident set) size of the process (in 1K byte units)
LIM	Soft limit on memory used. If no limit has been specified, it is shown as xx. If the limit is set to the system limit, a value of UNLIM is displayed.
TSIZ	Size of text (shared program) image
TRS	Size of resident (real memory) set of text
%CPU	CPU utilization of the process. Since the time base over which this is computed varies it is possible for the sum of all %CPU fields to exceed 100%.
%MEM	Percentage of real memory used by this process
COMMAND	The full command name and its parameters. This field is truncated. Run List Process Commands from this menu to see the full process command name and parameters. Run List Processes from this menu to see just the process name.

Figure 11-54 on page 11-67 shows an example of View Process Status output.

PID	TTY	STAT	TIME	PGIN	SIZE	RSS	LIM	TSIZ	TRS	%CPU	%MEM	COMMAND
0	-	S	0:41	6	8	8	xx	0	0	0.0	0.0	swapper
1	-	S	1:23	39	228	276	xx	21	24	0.1	1.0	/etc/init
514	-	R	1772:44	0	12	8	xx	0	0	0.0	0.0	kproc
771	-	S	2:10	0	16	16	xx	0	0	0.0	0.0	kproc
1028	-	S	0:00	0	16	16	xx	0	0	0.0	0.0	kproc
1521	-	S	0:31	68	452	536	xx	243	176	0.0	2.0	/usr/sbin/
1577	-	S	2:42	54	2640	3184	xx	63	488	0.2	11.0	/etc/sysmo
2149	-	S	0:00	0	16	12	xx	0	0	0.0	0.0	kproc
2359	-	S	0:49	7	96	136	xx	20	28	0.0	0.0	/etc/monpr
2570	-	S	0:22	16	48	44	xx	1	4	0.0	0.0	/etc/syncd
2872	-	S	0:26	24	96	136	xx	6	12	0.0	0.0	/etc/mondi
3303	-	S	0:08	2	40	48	xx	4	8	0.0	0.0	/etc/cfgdp
3340	-	S	0:52	90	212	244	xx	39	44	0.0	1.0	/usr/lib/e
3635	-	S	0:04	14	128	156	32768	16	24	0.0	1.0	/etc/syslo
3958	-	S	0:00	0	16	16	xx	0	0	0.0	0.0	kproc
4324	0	S	0:00	4	108	384	32768	303	276	0.0	1.0	-ksh
4417	-	S	0:30	48	148	232	xx	24	32	0.0	1.0	/etc/cron
4648	-	S	0:00	12	176	244	xx	21	28	0.0	1.0	/etc/srcms
4914	0	R	0:00	0	112	188	32768	34	48	0.0	1.0	/bin/ps gv
5179	-	S	0:17	37	320	464	xx	79	108	0.0	2.0	/etc/rt66c
5436	-	S	10:15	23	188	284	xx	54	80	0.6	1.0	/etc/scram
5693	-	S	0:00	5	68	100	xx	15	20	0.0	0.0	/etc/t960l
5950	-	S	0:00	13	152	208	32768	26	36	0.0	1.0	/etc/inetd
6629	-	S	0:24	65	268	452	xx	205	152	0.0	2.0	/usr/sbin/
6748	-	S	0:00	3	88	120	32768	11	8	0.0	0.0	/etc/write
7149	-	S	0:04	54	132	228	xx	226	120	0.0	1.0	/etc/ppp/l
7261	-	S	0:00	2	36	44	xx	4	8	0.0	0.0	/etc/uprin
7500	-	S	0:00	23	104	184	32768	41	52	0.0	1.0	/etc/qdaem
7723	-	S	0:00	0	48	72	xx	1	4	0.0	0.0	sleep 60
8178	-	S	0:08	137	488	672	xx	215	168	0.0	2.0	/usr/sbin/
8644	-	S	0:12	5	100	376	xx	303	276	0.0	1.0	ksh /etc/p
8934	-	S	0:02	10	144	96	xx	29	28	0.0	0.0	/etc/proto
9203	-	S	0:05	100	764	976	xx	266	228	0.0	3.0	/usr/sbin/
9460	-	S	0:12	70	708	888	xx	217	200	0.0	3.0	/usr/sbin/
9680	0	S	0:00	1	96	372	32768	303	276	0.0	1.0	ksh /usr/b
9941	0	R	0:10	101	1296	1536	32768	151	192	2.0	5.0	/usr/bin/s

Figure 11-54. Example of View Process Status Output

View Process Table Information

The process table maintains statistics on system variables, paging information, and file table information.

To view process table information using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View Process Information and Status** on the next menu.
3. Select **View Process Table Information** on the next menu.
4. Select a report destination (**screen** or **transfer_directory**) from the selector screen.
5. On the dialog screen, press **Tab** to select either **yes** or **no** to turn on or off each of the following process table options:
 - Display process table?
 - Display entries in the process table?

- Display file table?
- Display system variables?
- Display i-node information?
- Display paging information?

Figure 11-55 shows an example of View Process Table Information output.

SYSTEM VARS:

```

buffers    20
files      456
e_files    456
procs     131071
e_procs    48
c_lists   16384
maxproc    40
iostats     1
locks     200
e_locks   8522048

```

PROC TABLE:

SLT	ST	PID	PPID	PGRP	UID	EUID	PRI	CPU	EVENT	NAME
0	s	0	0	0	0	0	16	120		swapper
		FLAGS: swapped_in no_swap fixed_pri kproc wake/sig								
1	s	1	0	0	0	0	60	1		init
		FLAGS: swapped_in no_swap wake/sig locks								
2	r	202	0	0	0	0	127	120		wait
		FLAGS: swapped_in no_swap fixed_pri kproc								
3	s	303	0	0	0	0	39	0		netw
		FLAGS: swapped_in no_swap fixed_pri kproc								
4	s	404	0	0	0	0	36	0		netm
		FLAGS: swapped_in no_swap fixed_pri kproc								
5	s	5f1	629	629	0	0	60	0		snmpd
		FLAGS: swapped_in wake/sig								
6	s	629	1	629	0	0	60	0		sysmon
		FLAGS: swapped_in wake/sig								
8	s	865	1	75f	0	0	60	0		lvmb
		FLAGS: swapped_in kproc wake/sig								
9	s	937	629	629	0	0	60	0		monproc
		FLAGS: swapped_in remask wake/sig								
10	s	a0a	1	75f	0	0	60	0	0595b798	syncd
		FLAGS: swapped_in wake/sig								

Figure 11-55. Example of View Process Table Information Output

View Adapter Interface Statistics

The adapter interface statistics show network information gathered by these peer-capable adapters:

- Token-Ring Network 16/4 Adapter
- Ethernet Adapter
- EIA 422/449 Serial Adapter
- V.35/V.36 Serial Adapter.

The adapter interface name is used to access the adapter. See Table 11-4 for an explanation of the interface name.

Table 11-4. Adapter Interface Name Table

Adapter Name	Interface Name
Token-Ring Network 16/4 Adapter	tk#
Ethernet Adapter	te#
EIA 422/449 Serial Adapter	to?
V.35/V.36 Serial Adapter	to?

The number sign (#) can be a number from 0 through 6. The question mark (?) can be a number from 0 through 13. The number corresponds to the order of that particular interface type as it is located in the IBM 6611. For example, *te0* corresponds to the first Ethernet Adapter and *tk1* corresponds to the second Token-Ring Network 16/4 Adapter.

Figure 11-56 shows the menu screen for View Adapter Interface Statistics.

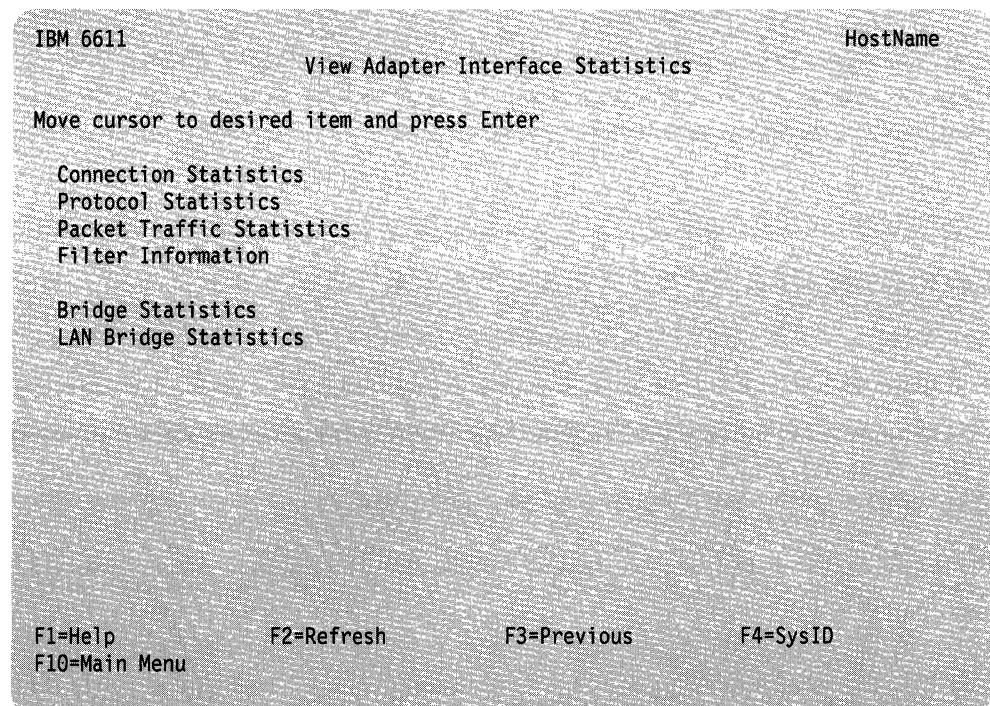


Figure 11-56. View Adapter Interface Statistics Menu

See these pages for more information about the individual menu items:

Connection Statistics	11-70
Protocol Statistics	11-71
Packet Traffic Statistics	11-72
Filter Information	11-73
Bridge Statistics	11-74
LAN Bridge Statistics	11-75

These tasks can be invoked using command primitives. See "Statistic-Gathering Command Primitives" on page 8-81 for information about the command primitives.

Connection Statistics

The adapter connection statistics lists the:

- Adapter interface
- Maximum transmission unit
- IP address for the interface.

To view connection statistics using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View Adapter Interface Statistics** on the next menu.
3. Select **Connection Statistics** on the next menu.
4. Select the adapter interface name for the adapter containing the connection statistics you want to view from the selector screen. See Table 11-4 on page 11-69 for an explanation of the interface name used to identify the adapters.
5. Select the protocol for which you want to view connection statistics from the next selector screen. The supported protocols are:
 - Internet
 - XNS
 - IPX
 - DECnet.
6. Select a report destination (**screen** or **transfer_directory**) from the next selector screen.

If you choose an adapter interface that is not enabled for the chosen protocol, no output is displayed with this command.

Figure 11-57 shows an example of Connection Statistics output for the Internet protocol.

Name	Mtu	Network	Address	Broadcast
lo0	1536	127	loopback	127.255.255.255
te1	1500	9.66.21	9.66.21.2	9.66.21.255
te0	1500	9.66.25	9.66.25.2	9.66.25.255
te2	1500	9.66.22	9.66.22.2	9.66.22.255
tk0	1500	9.66.23	9.66.23.2	9.66.23.255
to0	1500	9.66.2	9.66.2.2	

Figure 11-57. Example of Connection Statistics Output

Protocol Statistics

The adapter protocol statistics list the protocol statistics kept on the specified adapter for the specified protocol, either IP, IPX, XNS, or DECnet.

To view protocol statistics using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View Adapter Interface Statistics** on the next menu.
3. Select **Protocol Statistics** on the next menu.
4. Select the adapter interface name for the adapter containing the protocol statistics you want to view from the selector screen. See Table 11-4 on page 11-69 for an explanation of the interface name used to identify the adapters.
5. Select the protocol for which you want to view protocol statistics from the next selector screen. The protocols supported are:
 - Internet
 - XNS
 - IPX
 - DECnet.
6. Select a report destination (**screen** or **transfer_directory**) from the next selector screen.

If you choose an adapter interface that is not enabled for the chosen protocol, no output is displayed with this command.

Figure 11-58 on page 11-72 shows an example of Protocol Statistics output for the Internet protocol.

```
ip:
    ocIpForwarding = 1
    ocIpDefaultTTL = 255
    ocIpInReceives = 0
    ocIpInHdrErrors = 0
    ocIps_toosmall = 0
    ocIps_badver = 0
    ocIps_badhlen = 0
    ocIps_badsum = 0
    ocIps_badlen = 0
    ocIps_tooshort = 0
    ocIps_badttl = 0
    ocIpInAddrErrors = 0
    ocIpForwDatagrams = 0
    ocIpInUnknownProtos = 0
    ocIpInDiscards = 0
    ocIpInDelivers = 0
    ocIpOutRequests = 0
    ocIpOutDiscards = 0
    ocIpOutNoRoutes = 0
    ocIpReasmTimeout = 0
    ocIpReasmReqds = 0
    ocIpReasmOKs = 0
    ocIpReasmFails = 0
    ocIpFragOKs = 0
    ocIpFragFails = 0
    ocIpFragCreates = 0
    ocIpRoutingDiscards = 0
icmp:
    ocIcmpInMsgs = 0
    ocIcmpInErrors = 0
    ocIcps_tooshort = 0
    ocIcps_badlen = 0
    ocIcps_checksum = 0
    ocIcmpOutMsgs = 0
    ocIcmpOutErrors = 0
    ocIcps_squelched = 0
    Output histogram:
    Input histogram:
```

Figure 11-58. Example of Protocol Statistics Output

Packet Traffic Statistics

The adapter interface keeps counters on various network parameters. The statistics for packet counts are gathered here. They are displayed on the screen every few seconds, depending on the interval value.

To view packet traffic statistics using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View Adapter Interface Statistics** on the next menu.
3. Select **Packet Traffic Statistics** on the next menu.
4. Select the adapter interface name for the statistical data you want to view from the selector screen. See Table 10-1 on page 10-8 for an explanation of the interface name used to identify the adapters.
5. Select a report destination (**screen** or **transfer_directory**) from the next selector screen.
6. Enter **Number of seconds between displays** on the dialog screen.
7. Press **Ctrl + C** to end this command.

Figure 11-59 shows an example of Packet Traffic Statistics output. If the adapter interface name listed next to *Interface statistics:* in the header of the output is *lo0* or *lo1*, then the adapter interface you have chosen is not physically enabled.

```
Interface statistics: te0
Ipkts  Opkts  Epkts  Isys   Osys   Esys   Iptp   Optp   Eptp
  0      0      0    196    197      0      0      0      0
  0      0      0      1      1      0      0      0      0
  0      0      0      1      1      0      0      0      0
  0      0      0      1      1      0      0      0      0
  0      0      0      1      1      0      0      0      0
```

Figure 11-59. Example of Packet Traffic Statistics Output

Filter Information

The adapter filter information lists the configured filters for the specified protocol.

To view adapter filter information using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View Adapter Interface Statistics** on the next menu.
3. Select **Filter Information** on the next menu.
4. Select the adapter interface name for the statistical data you want to view from the selector screen. See Table 11-4 on page 11-69 for an explanation of the interface name used to identify the adapters.
5. Select the protocol for which you want to view filter information from the next selector screen. The supported protocols are:
 - Internet
 - XNS
 - IPX
 - DECnet
6. Select a report destination (**screen** or **transfer_directory**) from the next selector screen.

If you choose an adapter interface that is not enabled for the chosen protocol, no output is displayed with this command.

An example of the output for DECnet is in Figure 11-60 on page 11-74.

DECnet Filters for interface tk0

State of all DECnet Filters for interface tk0: Disabled
Number of DECnet Filters for interface tk0: 3

Id	Direction	Action	Type	Address1	Mask1	[Address2]	[Mask2]
10	Inbound	Permit	Dual	1.1	63.1023		
20	Outbound	Permit	Singular	2.2	63.1023		
40	Inbound	Deny	singular	3.3	63.1023		

Figure 11-60. Example of Filter Information Output for DECnet

Bridge Statistics

The bridge statistics display counters for various network parameters kept on the peer-capable adapters. These are useful for solving problems with the bridge protocol. They are displayed on the screen every few seconds, depending on the interval value.

To view bridge statistics using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View Adapter Interface Statistics** on the next menu.
3. Select **Bridge Statistics** on the next menu.
4. Select the adapter interface name for the statistical data you want to view from the selector screen. See Table 11-4 on page 11-69 for an explanation of the interface name used to identify the adapters.

Only the Token-Ring Network 16/4 Adapters, EIA 422/449 Serial Adapters, and V.35/V.36 Serial Adapters are supported with this function.

5. Select a report destination (**screen** or **transfer_directory**) from the next selector screen.
6. Enter **Number of seconds between displays** on the dialog screen.
7. Press **Ctrl + C** to end this command.

If you choose an adapter interface that is not enabled for bridging, there is no output displayed with this command. However, you still need to press **Ctrl + C** to end the command.

Figure 11-61 shows an example of Bridge Statistics output.

iSPEC	oSPEC	iARB	oARB	iSRB	oSRB	MTU	Dups	Mismatch
9	18	9	9	0	0	0	0	0
1	2	2	2	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Figure 11-61. Example of Bridge Statistics Output

LAN Bridge Statistics

The LAN bridge statistics display counters for various network parameters kept on the EIA 422/449 Serial Adapter or the V.35/V.36 Serial Adapter. These are useful for solving problems with the LAN bridge protocol. They are displayed on the screen every few seconds depending on the interval value.

To view LAN bridge statistics using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View Adapter Interface Statistics** on the next menu.
3. Select **LAN Bridge Statistics** on the next menu.
4. Select the adapter interface name for the statistical data you want to view from the selector screen. See Table 11-4 on page 11-69 for an explanation of the interface name used to identify the adapters.

The LAN bridge protocol is only supported on the EIA 422/449 Serial Adapters and the V.35/V.36 Serial Adapters.

5. Select a report destination (**screen** or **transfer_directory**) from the next selector screen.
6. Enter **Number of seconds between displays** on the dialog screen.
7. Press **Ctrl + C** to end this command.

If you choose an adapter interface that is not enabled for LAN bridging, there is no output displayed with this command. However, you still need to press **Ctrl + C** to end the command.

Figure 11-62 shows an example of LAN Bridge Statistics output.

iWire	oWire	i2Sec	i4Sec	o4Sec	e4Sec	i1pf	o1pf	iSys	oSys	Act	Link
672	10153	10112	672	9753	37	0	0	0	0	1	1
0	0	0	0	0	0	0	0	0	0	1	1
0	0	0	0	0	0	0	0	0	0	1	1
0	0	0	0	0	0	0	0	0	0	1	1
0	0	0	0	0	0	0	0	0	0	1	1

Figure 11-62. Example of LAN Bridge Statistics Output

View System Network Statistics

Figure 11-63 on page 11-76 shows the menu screen for View System Network Statistics. System network statistics are those network parameters that are gathered by the base operating system, as opposed to the peer-capable adapters. Some packets are forwarded by the adapters bypassing the base operating system.

With some of these statistics, the adapter interfaces are listed. The adapter interface names are explained in Table 11-5 on page 11-76.

Table 11-5. Adapter Interface Name Table

Adapter Name	Interface Name
Token-Ring Network 16/4 Adapter	tk#
Ethernet Adapter	te#
EIA 422/449 Serial Adapter	to?
V.35/V.36 Serial Adapter	to?
X.25 Adapter	xt#
Loopback	lo\$

The number sign (#) can be a number from 0 to 6. The question mark (?) can be a number from 0 to 13. The dollar sign (\$) is either 0 or 1. The number corresponds to the order of that particular interface type as it is located in the IBM 6611. For example, *te0* corresponds to the first Ethernet adapter and *tk1* corresponds to the second Token Ring adapter.

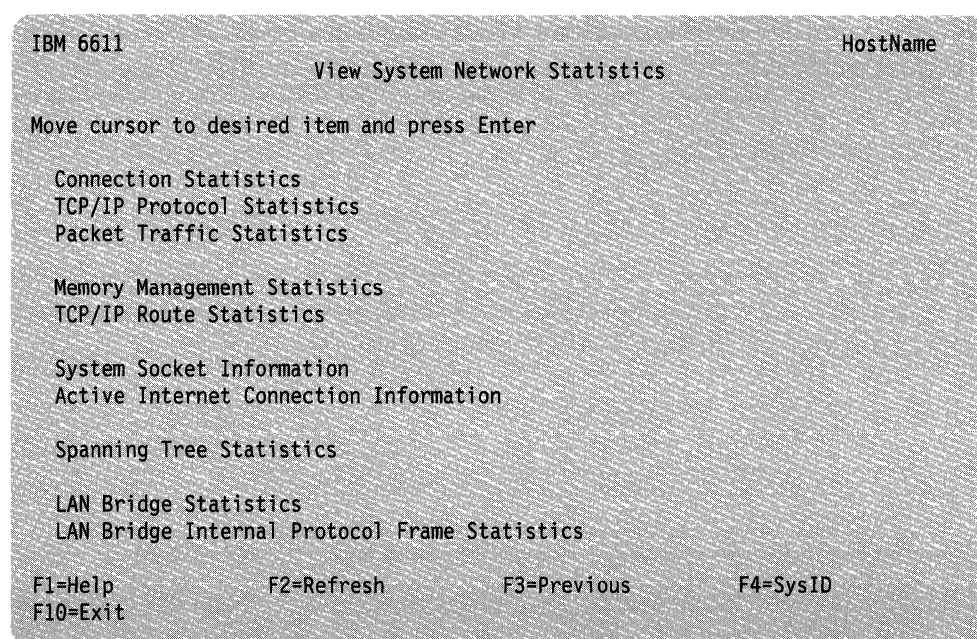


Figure 11-63. View System Network Statistics Menu

See these pages for more information about the individual menu items:

Connection Statistics	11-77
TCP/IP Protocol Statistics	11-77
Packet Traffic Statistics	11-79
Memory Management Statistics	11-80
TCP/IP Route Statistics	11-80
System Socket Information	11-81
Active Internet Connection Information	11-81
Spanning Tree Statistics	11-82
LAN Bridge Statistics	11-85
LAN Bridge Internal Protocol Frame Statistics	11-86

These tasks can be invoked using command primitives. See “Statistic-Gathering Command Primitives” on page 8-81 for information about the command primitives.

Connection Statistics

The system network connection statistics list:

- Maximum transmission unit
- Inbound packets and errors
- Outbound packets and errors.

To view connection statistics using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View System Network Statistics** on the next menu.
3. Select **Connection Statistics** on the next menu.
4. Select a report destination (**screen** or **transfer_directory**) from the selector screen.

Figure 11-64 shows an example of Connection Statistics output. If you receive an asterisk (*) beside any of the listed interface names, this is an indication that the adapter or port is not enabled.

Name	Mtu	Network	Address	Ipkts	Ierrs	Opkts	Oerrs	Coll
lo0	1536	<Link>		8945	0	8945	0	0
lo0	1536	loopback	loopback	8945	0	8945	0	0
to0	1500	<Link>		3861	0	4238	0	0
to0	1500	8.8.8	8.8.8.1	3861	0	4238	0	0
to1*	1500	<Link>		13	0	15	0	0
te0	1500	<Link>		10833	0	7716	0	0
te0	1500	9.66.31	9.66.31.10	10833	0	7716	0	0
te0	1500	ns:23H	8005A1324C9H	10833	0	7716	0	0
te0	1500	ipx:1997H	8005A1324C9H	10833	0	7716	0	0
te1	1500	<Link>		335	0	3951	0	0
te1	1500	DECnet	25.25	335	0	3951	0	0

Figure 11-64. Example of Connection Statistics Output

TCP/IP Protocol Statistics

The base operating system maintains statistics on the following TCP/IP protocols:

- IP
- TCP
- UDP
- ICMP.

To view TCP/IP protocol statistics using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View System Network Statistics** on the next menu.
3. Select **TCP/IP Protocol Statistics** on the next menu.
4. Select one of the following protocols for which you want to view statistics from the next selector screen:
 - IP
 - TCP
 - UDP
 - ICMP
 - TCP/IP.

5. Select a report destination (**screen** or **transfer_directory**) from the selector screen.

Figure 11-65 shows an example of TCP/IP Protocol Statistics output when TCP/IP is chosen.

```
ip:      10513 total packets received
         0 bad header checksums
         0 with size smaller than minimum
         0 with data size < data length
         0 with header length < data size
         0 with data length < header length
         0 fragments received
         0 fragments dropped (dup or out of space)
         0 fragments dropped after timeout
         0 packets forwarded
         0 packets not forwarded
         0 redirects sent

icmp:    12 calls to icmp_error
         0 errors not generated
         Output histogram:
             address mask reply: 1
         0 messages with bad code fields
         0 messages < minimum length
         0 bad checksums
         0 messages with bad length
         Input histogram:
             echo reply: 7
             address mask request: 1
         1 message response generated

tcp:     5166 packets sent
         3514 data packets (107338 bytes)
         0 data packets (0 bytes) retransmitted
         1304 ack-only packets (783 delayed)
         0 URG only packets
         0 window probe packets
         0 window update packets
         348 control packets
```

Figure 11-65 (Part 1 of 2). Example of TCP/IP Protocol Statistics Output

```

5221 packets received
    3862 acks (for 107686 bytes)
    175 duplicate acks
    0 acks for unsent data
    3629 packets (107338 bytes) received in-sequence
    55 completely duplicate packets (0 bytes)
    0 packets with some dup. data (0 bytes duped)
    115 out-of-order packets (0 bytes)
    0 packets (0 bytes) of data after window
    0 window probes
    1 window update packet
    0 packets received after close
    0 discarded for bad checksums
    0 discarded for bad header offset fields
    0 discarded because packet too short
118 connection requests
118 connection accepts
236 connections established (including accepts)
232 connections closed (including 0 drops)
0 embryonic connections dropped
3980 segments updated rtt (of 3980 attempts)
0 retransmit timeouts
    0 connections dropped by rexmit timeout
0 persist timeouts
55 keepalive timeouts
    55 keepalive probes sent
    0 connections dropped by keepalive
udp:
    0 incomplete headers
    0 bad data length fields
    0 bad checksums

```

Figure 11-65 (Part 2 of 2). Example of TCP/IP Protocol Statistics Output

Packet Traffic Statistics

The main operating system keeps counters on various network parameters for the adapter interfaces. The statistics for packet counts are gathered here. They are displayed on the screen every few seconds, depending on the interval value.

To view packet traffic statistics using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View System Network Statistics** on the next menu.
3. Select **Packet Traffic Statistics** on the next menu.
4. Select an interface name from the selector screen. See Table 11-5 on page 11-76 for an explanation about the interface name used to identify the adapters.
5. Select a report destination (**screen** or **transfer_directory**) from the selector screen.
6. Enter the number of seconds between displays on the dialog screen.
7. Press **Ctrl + C** to end this command.

Figure 11-66 on page 11-80 shows an example of Packet Traffic Statistics output.

input (te0)			output			input (Total)			output		
packets	errs	packets	errs	colls	packets	errs	packets	errs	packets	errs	colls
208	0	208	0	0	11428	0	11411	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0

Figure 11-66. Example of Packet Traffic Statistics Output

Memory Management Statistics

These statistics show base operating system memory management information.

To view memory management statistics using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View System Network Statistics** on the next menu.
3. Select **Memory Management Statistics** on the next menu.
4. Select a report destination (**screen** or **transfer_directory**) from the selector screen.

Figure 11-67 shows an example of Memory Management Statistics output.

```

554 mbufs in use:
    80 mbufs allocated to data
    6 mbufs allocated to packet headers
    192 mbufs allocated to socket structures
    238 mbufs allocated to protocol control blocks
    14 mbufs allocated to routing table entries
    18 mbufs allocated to socket names and addresses
    6 mbufs allocated to interface addresses
    6 mbufs allocated to <mbuf type 17>
80/101 mapped pages in use
542 Kbytes allocated to network (84% in use)
0 requests for memory denied
0 requests for memory delayed
0 calls to protocol drain routines

```

Figure 11-67. Example of Memory Management Statistics Output

TCP/IP Route Statistics

These statistics show routing information about the TCP/IP routing protocols.

To view TCP/IP route statistics using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View System Network Statistics** on the next menu.
3. Select **TCP/IP Route Statistics** on the next menu.
4. Select a report destination (**screen** or **transfer_directory**) from the selector screen.

Figure 11-68 on page 11-81 shows an example of TCP/IP Route Statistics output.

routing:

0 bad routing redirects
0 dynamically created routes
0 new gateways due to redirects
0 destinations found unreachable
0 uses of a wildcard route

Figure 11-68. Example of TCP/IP Route Statistics Output

System Socket Information

To view system socket information using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View System Network Statistics** on the next menu.
3. Select **System Socket Information** on the next menu.
4. Select a report destination (**screen** or **transfer_directory**) from the selector screen.

Figure 11-69 shows an example of System Socket Information output.

Active domain sockets								
SADR/PCB	Type	Recv-Q	Send-Q	Inode	Conn	Refs	Nextref	
54f0a14	stream	0	0	5840928	0	0	0	/tmp/sysmon.action
54f0b14								
54f0c14	stream	0	0	0	54ef114	0	0	
54ef514								
54e3014	dgram	0	0	5840108	0	0	0	/dev/SRC
54f0014								
54f0d14	stream	0	0	0	54ef514	0	0	
54ef114								
54ee114	stream	0	0	0	54ee414	0	0	
54ee214								
54ef414	stream	0	0	0	54ef714	0	0	
54ef014								
54ee314	stream	0	0	0	54ee214	0	0	
54ee414								
54ef314	dgram	0	0	5840a60	0	0	0	/dev/.SRC-unix/SRCEigCnm
54f0e14								
54eea14	stream	0	0	0	54eed14	0	0	

Figure 11-69. Example of System Socket Information Output

Active Internet Connection Information

These statistics show active internet connections.

To view active internet connection information using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View System Network Statistics** on the next menu.
3. Select **Active Internet Connection Information** on the next menu.
4. Select whether to include server processes on the selector screen.
5. Select a report destination (**screen** or **transfer_directory**) from the next selector screen.

Figure 11-70 shows an example of Active Internet Connection Information output.

Active Internet connections						
PCB/ADDR	Proto	Recv-Q	Send-Q	Local Address	Foreign Address	(state)
552c014	tcp	0	0	u2.telnet	glc.1054	ESTABLISHED

Figure 11-70. Example of Active Internet Connection Information Output

Spanning Tree Statistics

Spanning tree statistics can be gathered for both source route bridging and transparent bridging.

Source Route Bridge Spanning Tree Statistics: These statistics show traffic and error statistics for the spanning tree protocol.

To view spanning tree statistics using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View System Network Statistics** on the next menu.
3. Select **Spanning Tree Statistics** on the next menu.
4. Select **Source Route Bridge Spanning Tree Statistics** on the next menu.
5. Select an interface name from the selector screen. See Table 11-4 on page 11-69 for an explanation about the interface name used to identify the adapters.

Only the Token-Ring Network 16/4 Adapters, V.35/V.36 Serial Adapters, and the EIA 422/449 Serial Adapters are supported with this function.

6. Select a report destination (**screen** or **transfer_directory**) from the next selector screen.
7. Enter the number of seconds between displays on the dialog screen.
8. Press **Ctrl + C** to end this command.

If you choose an adapter interface that is not enabled for spanning tree, there is no output displayed with this command. However, you still need to press **Ctrl + C** to end the command.

Figure 11-71 shows an example of Source Route Bridge Spanning Tree Statistics output.

iBpdu	oBpdu	iTcn	oTcn	iError	oError	state	flag
0	9816	0	0	0	0	FRW	ON
0	1	0	0	0	0	FRW	ON
0	1	0	0	0	0	FRW	ON
0	1	0	0	0	0	FRW	ON
0	1	0	0	0	0	FRW	ON

Figure 11-71. Example of Source Route Bridge Spanning Tree Statistics Output

Source Route Bridge Spanning Tree Frame Relay Statistics: These statistics show packet traffic and errors for the spanning tree protocol running on frame relay.

To view spanning tree frame relay statistics using the System Manager:

1. Select **Performance and Statistics** from the main menu.

2. Select **View System Network Statistics** on the next menu.
3. Select **Spanning Tree Statistics** on the next menu.
4. Select **Source Route Bridge Spanning Tree Frame Relay Statistics** on the next menu.
5. Select an interface name from the selector screen. See Table 11-4 on page 11-69 for an explanation about the interface name used to identify the adapters.

This function is only supported on the EIA 422/449 Serial Adapters and the V.35/V.36 Serial Adapters.

6. Select a report destination (**screen** or **transfer_directory**) from the next selector screen.
7. Enter the number of seconds between displays on the dialog screen.
8. Select the port index on the dialog screen. Press **F4 (Esc + 4)** on the entry field and press **Enter** to get a port index from the pop-up list.

If you choose an adapter interface that does not have spanning tree and frame relay enabled, the command will be suspended when you press **F4 (Esc + 4)** to list the port indexes. The bottom of the dialog screen will have the *Processing data ...* message as shown below.

F1=Help	F2=Refresh	F3=Previous	F4=List
F5=Undo			
F10=Exit	Processing data ...		

Press **Ctrl + C** to end the suspension.

9. Press **Ctrl + C** to end this command.

Figure 11-72 shows an example of Source Route Bridge Spanning Tree Frame Relay Statistics output.

iBpdu	oBpdu	iTcn	oTcn	iError	oError	state	flag
0	0	0	0	0	0	LIS	DOWN
0	0	0	0	0	0	LIS	DOWN
0	0	0	0	0	0	LIS	DOWN
0	0	0	0	0	0	LIS	DOWN
0	0	0	0	0	0	LIS	DOWN
0	0	0	0	0	0	LIS	DOWN

Figure 11-72. Example of Source Route Bridge Spanning Tree Frame Relay Statistics Output

Transparent Bridge Spanning Tree Statistics: These statistics show traffic and error statistics for the spanning tree protocol.

To view spanning tree statistics using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View System Network Statistics** on the next menu.
3. Select **Spanning Tree Statistics** on the next menu.
4. Select **Transparent Bridge Spanning Tree Statistics** on the next menu.

5. Select an interface name from the selector screen. See Table 11-4 on page 11-69 for an explanation about the interface name used to identify the adapters.

Only the Token-Ring Network 16/4 Adapters, V.35/V.36 Serial Adapters, and the EIA 422/449 Serial Adapters are supported with this function.

6. Select a report destination (**screen** or **transfer_directory**) from the next selector screen.
7. Enter the number of seconds between displays on the dialog screen.
8. Press **Ctrl + C** to end this command.

If you choose an adapter interface that is not enabled for spanning tree, there is no output displayed with this command. However, you still need to press **Ctrl + C** to end the command.

Figure 11-73 shows an example of Transparent Bridge Spanning Tree Statistics output.

iBpdu	oBpdu	iTcn	oTcn	iError	oError	state
0	9816	0	0	0	0	FRW
0	1	0	0	0	0	FRW
0	1	0	0	0	0	FRW
0	1	0	0	0	0	FRW
0	1	0	0	0	0	FRW

Figure 11-73. Example of Transparent Bridge Spanning Tree Statistics Output

Transparent Bridge Spanning Tree Frame Relay Statistics: These statistics show packet traffic and errors for the spanning tree protocol running on frame relay.

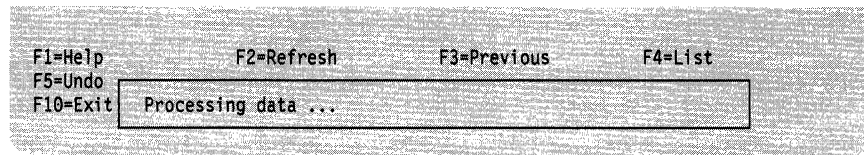
To view spanning tree frame relay statistics using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View System Network Statistics** on the next menu.
3. Select **Spanning Tree Statistics** on the next menu.
4. Select **Transparent Bridge Spanning Tree Frame Relay Statistics** on the next menu.
5. Select an interface name from the selector screen. See Table 11-4 on page 11-69 for an explanation about the interface name used to identify the adapters.

This function is only supported on the EIA 422/449 Serial Adapters and V.35/V.36 Serial Adapters.

6. Select a report destination (**screen** or **transfer_directory**) from the next selector screen.
7. Enter the number of seconds between displays on the dialog screen.
8. Select the port index on the dialog screen. Press **F4 (Esc + 4)** on the entry field and press **Enter** to select a port index from the port index pop-up list.

If you choose an adapter interface that does not have spanning tree and frame relay enabled, the command will be suspended when you press **F4 (Esc + 4)** to list the port indexes. The bottom of the dialog screen will have the *Processing data ...* message as shown below.



Press **Ctrl + C** to end the suspension.

9. Press **Ctrl + C** to end this command.

Figure 11-74 shows an example of Transparent Bridge Spanning Tree Frame Relay Statistics output.

iBpdu	oBpdu	iTcn	oTcn	iError	oError	state
0	0	0	0	0	0	LIS
0	0	0	0	0	0	LIS
0	0	0	0	0	0	LIS

Figure 11-74. Example of Transparent Bridge Spanning Tree Frame Relay Statistics Output

LAN Bridge Statistics

These statistics show traffic and error statistics for the LAN bridge protocol.

To view LAN bridge statistics using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View System Network Statistics** on the next menu.
3. Select **LAN Bridge Statistics** on the next menu.
4. Select an interface name on the selector screen. See Table 11-4 on page 11-69 for an explanation of the interface name used to identify the adapters.

The LAN bridge protocol is only supported on the EIA 422/449 Serial Adapters and the V.35/V.36 Serial Adapters.

5. Select a report destination (**screen** or **transfer_directory**) from the next selector screen.
6. Enter the number of seconds between displays on the dialog screen.
7. Press **Ctrl + C** to end this command.

If you choose an adapter interface that is not enabled for LAN bridging, there is no output displayed with this command. However, you still need to press **Ctrl + C** to end the command.

Figure 11-75 on page 11-86 shows an example of LAN Bridge Statistics output.

iIpF	oIpF	iAck	oAck	o2Sec	oRetry	iError	oError	Active	Link
672	10153	10112	672	9753	37	0	0	1	1
0	0	0	0	0	0	0	0	1	1
0	1	1	0	1	0	0	0	1	1
0	1	1	0	1	0	0	0	1	1
0	1	1	0	1	0	0	0	1	1
0	1	1	0	1	0	0	0	1	1
0	1	1	0	1	0	0	0	1	1

Figure 11-75. Example of LAN Bridge Statistics Output

LAN Bridge Internal Protocol Frame Statistics

These statistics show internal frames for the LAN bridge protocol.

To view LAN bridge internal protocol frame statistics using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **View System Network Statistics** on the next menu.
3. Select **LAN Bridge Internal Protocol Frame Statistics** on the next menu.
4. Select an interface name on the selector screen. See Table 11-4 on page 11-69 for an explanation of the interface name used to identify the adapters.

The LAN bridge protocol is only supported on the EIA 422/449 Serial Adapters and V.35/V.36 Serial Adapters.

5. Select a report destination (**screen** or **transfer_directory**) from the next selector screen.
6. Enter the number of seconds between displays on the dialog screen.
7. Press **Ctrl + C** to end this command.

If you choose an adapter interface that is not enabled for LAN bridging, there is no output displayed with this command. However, you still need to press **Ctrl + C** to end the command.

Figure 11-76 on page 11-87 shows an example of LAN Bridge Internal Protocol Frame Statistics output.

```

IPF recv <- INIT(3),ADAPTINFO(3),RINGSTATUS,PERFCNTREQ(327),
PERPERFCNT(326),TERMINATE,SELFTESTSTART(3),LLCXMIT(8),
IPF sent -> INIT(4),CONFIG(3),ADAPTINFO(3),PERFCNTRES(327),TERMINATE,
SELFTESTSTART(3),SPTHELLO(9832),
*
IPF recv <-
IPF sent -> SPTHELLO,
*
IPF recv <-
IPF sent -> SPTHELLO,
*
IPF recv <- PERFCNTREQ,PERPERFCNT,
IPF sent -> PERFCNTRES,SPTHELLO,
*
IPF recv <-
IPF sent -> SPTHELLO,
*
IPF recv <-
IPF sent -> SPTHELLO,
*

```

Figure 11-76. Example of LAN Bridge Internal Protocol Frame Statistics Output

View Virtual Memory Statistics

This task reports statistics about processes, virtual memory, disks, traps, and CPU activity. Without any options, the report contains a summary of the virtual memory activity since the system was started.

The interval parameter specifies the amount of time between reports. The first report contains statistics from the time the system started. Subsequent reports contain statistics collected from the end of the last interval that was reported. If the interval option is not specified, the task generates a single report and exits.

To view virtual memory statistics using the System Manager:

1. Log in with a controlling userid.
2. Select **Performance and Statistics** from the main menu.
3. Select **View System Network Statistics** on the next menu.
4. Select **View Virtual Memory Statistics** on the next menu.
5. Select a report destination (**screen** or **transfer_directory**) from the selector screen.
6. Enter **Seconds between samples** and **Number of samples** on the dialog screen.

Figure 11-77 shows an example of View Virtual Memory Statistics output.

procs		memory			page				faults				cpu			
r	b	avm	fre	re	pi	po	fr	sr	cy	in	sy	cs	us	sy	id	wa
0	0	5441	91	0	0	0	0	0	0	111	69	22	1	1	97	1
0	0	5441	91	0	0	0	0	0	0	212	277	166	4	5	91	0

Figure 11-77. Example of View Virtual Memory Statistics Output

View Input/Output Statistics

This task is used to monitor system input and output device loading. It generates statistical reports for the terminal and disk devices.

The first report generated by this menu item provides statistics concerning the time since the system was started. Each subsequent report covers the time since the previous report. All statistics are reported each time this task is invoked.

To view I/O statistics using the System Manager:

1. Login with a controlling userid.
2. Select **Performance and Statistics** from the main menu.
3. Select **View System Network Statistics** on the next menu.
4. Select **View Input/Output Statistics** on the next menu.
5. Select a report destination (**screen** or **transfer_directory**) from the selector screen.
6. Enter **Seconds between samples** and **Number of samples** on the dialog screen.

Figure 11-78 shows an example of View Input/Output Statistics output.

tty:	tin	tout	cpu:	% user	% sys	% idle	% iowait
	0.0	3.1		0.5	1.1	97.1	1.2
Disks:	% tm_act	Kbps	tps	mtps	Kb_read	Kb_wrtn	
hdisk0	1.3	2.2	0.5		26912	215638	
hdisk1	0.1	0.2	0.0		3447	18368	
tty:	tin	tout	cpu:	% user	% sys	% idle	% iowait
	0.0	142.8		3.5	4.0	92.5	0.0
Disks:	% tm_act	Kbps	tps	mtps	Kb_read	Kb_wrtn	
hdisk0	0.0	0.0	0.0		0	0	
hdisk1	0.0	0.0	0.0		0	0	

Figure 11-78. Example of View Input/Output Statistics Output

Export Performance Data

To export performance data using the System Manager:

1. Select **Performance and Statistics** from the main menu.
2. Select **Export Performance Data** on the next menu.
3. Select an Export method from the selector screen.
 - FTP
 - Modem
 - DOS diskette
 - UNIX diskette.
4. With each of these file transfer methods, a selector screen appears requesting the name of the file to be transferred. Select the name of the performance data file.
 - Transferring files with FTP requires you to give the host name and a userid at the destination node on the dialog screen. You are prompted for the password for the userid.
 - Transferring files to a DOS diskette requires you to give the name of the file on the DOS diskette.
 - Transferring files to a UNIX diskette requires you to specify whether to *append* the file to the end of the diskette or to place it as the only file on the diskette, *create*.

Figure 11-79 shows an example of exporting the input/output statistics to a DOS diskette.

Free space: 1334564 bytes
The file ps_io.stat has been exported to ps_io.sta on the DOS diskette.

Figure 11-79. Example of Export Performance Data to DOS Diskette

Chapter 12. Using the Software Installation and Maintenance Facility

About This Chapter	12-2
Software Component and Update Packaging	12-2
Installing Software Changes	12-3
Installing Software Updates	12-3
Installing Software Components	12-5
Restarting System after Software Installation	12-6
Software Installation Procedure	12-6
Post Software Installation Functions	12-16
Clean Up After a Failed Installation	12-16
Commit Applied Updates (Delete Previous Version)	12-16
Reject Applied Updates (Use Previous Version)	12-17
Reinstate Saved Software Component	12-18
Remove Saved Software Component	12-18
Automating Software Installation and Maintenance Facility Functions	12-19
Sending Software Updates to One IBM 6611	12-19
Sending Software Updates to Multiple IBM 6611s	12-21
Sending Software Components to Multiple IBM 6611s	12-23
Transferring Software Changes to an IBM 6611	12-25
Transferring Software from a Diskette to an IBM 6611	12-26
Transferring Software from Diskette to the RISC System/6000 Workstation	12-27
Transferring Software from a RISC System/6000 Workstation to an IBM 6611 Using FTP	12-28
Transferring Software from an IBM 6611 to an IBM 6611 Using FTP	12-30
Transferring Software from a RISC System/6000 Workstation to an IBM 6611 Using Xmodem	12-32
Saving Your Software and Configuration Diskettes	12-33
Software Vital Product Data	12-33
List All Installed Software	12-35
List All Updates to a Software Component	12-35
List Files Included in a Software Component	12-36
List Prerequisites of a Software Component	12-36
List Dependents of a Software Component	12-37
View ID of a Software Component	12-38
View History of a Software Component	12-38
Verify a Software Component	12-39
Exporting the Software Vital Product Data	12-40

About This Chapter

This chapter describes the Software Installation and Maintenance Facility. This facility is used to install software components and software updates for the Multiprotocol Network Program. It is also a tracking utility that maintains status and history information about the Multiprotocol Network Program software. There is a multiphase commit and reject capability for software updates. This allows you to test specific software updates on the system for a period of time before you decide whether to make the changes permanent.

Software Component and Update Packaging

The Multiprotocol Network Program, with the exception of the Configuration Program, is preinstalled on the fixed disk of the IBM 6611 when you receive it. The Configuration Program is sent on diskettes that are stored with this book.

There are two types of software changes that are installed on the IBM 6611.

Software components

The networking software in the Multiprotocol Network Program is divided into two separately installable software components:

- mpnp.obj
- mpnp.data.

Software updates

When a problem is encountered in the Multiprotocol Network Program, files are changed to repair the software. These files are packaged together along with necessary installation information as a software update. A software update provides a fix to a particular software component. A software update is also called a *program temporary fix*, or *PTF*.

Software components and updates are installed using the Software Installation and Maintenance Facility.

You are asked to apply all software component packages that are sent to you. However, you can select the software updates that you want to install. You can apply all the software updates that are available or only those that affect your configuration.

Note: There may be an instance when a significant software update package is needed. IBM service personnel can request that all customers install the package.

The software updates are sent as self-contained packages with all of the information necessary to apply the update to the system. The software update includes:

- Update instructions
- Prerequisite and corequisite information
- Authorized Program Analysis Report (APAR) information
- Files containing fixed code.

Each software update contains instructions explaining how the update is installed on the system. This includes programs invoked during installation. In addition, information, such as the available memory required to apply the update, is imbedded within the update instructions.

Each software update also contains information about all updates that are prerequisite or corequisite. A prerequisite update must be applied to the

Multiprotocol Network Program before the installation of a software update, designating it as a prerequisite. Corequisite software updates must be applied during the same installation session. The Software Installation and Maintenance Facility ensures that the software updates are applied correctly using the prerequisite and corequisite information supplied. The software component to which the update is applied is a prerequisite of the software update.

The APAR information is also included to tell you the problems that are fixed by the software update. One software update can fix one or more APARs.

A software component contains all the files that are a part of that section of the Multiprotocol Network Program. When a new software component is installed, replacing an existing one, all knowledge of the former software component and its updates are removed. The new software component will generally be a superset of the software component and software updates that it replaces.

Installing Software Changes

A software package can contain software updates, software components, or both. If the software package contains both software components and updates, they need to be installed separately. The software components are installed first if the software updates belong to the new software component. The software updates are installed first if the software updates belong to the previous software component. However, if the updates belong to the previous component and you are going to install the new component immediately after installing the updates, the only reason to install the updates at all would be to have them as part of the previous component, when it is saved.

The Software Installation and Maintenance Facility is accessed using:

- The System Manager
- The command primitives in the fast-path environment
- The **rexec** or **rsh** commands.

Only a controlling user can issue most of the commands in the Software Installation and Maintenance Facility.

IBM recommends that you use the System Manager for software installation of individual IBM 6611s. If you manage your software installation from a central location and update each of your IBM 6611s at the same time, there are two scripts that are sent with the Multiprotocol Network Program that are used to automate the process of applying software changes to multiple IBM 6611s. One is for software updates or PTFs and one is for software components. You can also write your own RSH automation scripts using the install primitives. See “Automating Software Installation and Maintenance Facility Functions” on page 12-19 for information about using automation scripts for installing software changes.

Installing Software Updates

Software updates are installed using the Software Installation and Maintenance Facility of the Multiprotocol Network Program. This is a multiphase process that permits the software updates to be tested before making them a permanent part of the Multiprotocol Network Program.

When software updates are first installed, they are **applied** to the system. The files that are replaced by the software update are saved, in case you want to **reject** the software update. The **applied** update becomes part of the running system and can

be tested. The files are saved until you **commit** the software update. When you **commit** the software update, the saved files are deleted, eliminating the possibility of returning to the previous version. If you **reject** the applied, but not committed, software update, the saved files are restored and the applied update files are deleted. You cannot **reject** a software update that has been **committed**.

Warning: When you **commit** the software update, the change is permanent.

There are several rules to consider when installing software updates that have dependencies:

- Software updates cannot be applied until their base component is applied.
- Software updates cannot be applied until their prerequisite software updates have been applied.
- Corequisite software updates must be applied during the same installation step.
- Applied software updates cannot be committed until their prerequisite software updates have been committed.
- Corequisite software updates must be committed during the same installation step.

During the installation process, status and error messages are written to the screen. If the installation fails, an indication of why it failed should be displayed on the screen. If failures are detected or, if the installation process is interrupted, the Software Installation and Maintenance Facility attempts to “clean up” by removing software updates that were partially installed and restoring the component to its state before attempting to install the software update.

In most cases the Software Installation and Maintenance Facility’s automatic cleanup is successful. Normally, the only scenario when you must perform a manual cleanup is when the system shuts down or loses power during the installation. If you have a problem with your installation that results in a partial installation and the automatic “cleanup” is not successful, select **Clean Up After a Failed Installation** to clean up the partial installation and restore the saved file.

If the system successfully returns to the previous state, that version of the component becomes the current version. If this cannot be done, the software component is marked as broken. IBM recommends that you reinstall any broken software components.

A summary report is provided at the end of the installation step that lists the status of each of the software updates that were installed.

The installation of software updates can fail for several reasons:

1. There is insufficient space in the file system where the saved files are stored, when the update is applied. To create more space, you can:
 - Commit applied software updates.
 - Remove the saved software component.
2. The software update failed its verification during the install step. The software update files were corrupted during the transfer to the IBM 6611. You can attempt to recover by applying the software updates directly from the diskette or resending them.
3. Software updates that are a prerequisite to the one being applied have not already been applied and are not part of the software package being applied. Software updates that are a corequisite to the one being applied are not part of the software package being applied.

When installing software updates from the transfer directory, the software update images are removed from the directory after installation.

Installing Software Components

Software components are installed using the Software Installation and Maintenance Facility of the Multiprotocol Network Program. When a new software component is installed replacing an existing one, all knowledge of the previous software component and its updates is removed. All the software files are overlaid. The software vital product data does not show the existence of the previous software component. However, the previous component and all its installed updates are saved.

All uncommitted software updates for the previous software component must be either committed or rejected before the installation of the new software component. If this is not done, you will receive an error message when you attempt to install the new component.

During the installation process, status and error messages are written to the terminal. If the installation fails, an indication of why should be displayed on the terminal.

A summary report is provided at the end of the installation step that lists the status of each of the software components that were installed.

The installation of software components can fail for several reasons:

1. There is insufficient space in the file system where the saved component is stored, when the new component is applied. When this occurs, you are asked whether or not you want to continue with the component installation without saving the existing component. If you choose to abruptly end the installation, you can create more space to save the existing software component by committing applied software updates.
2. The software component failed its verification during the installation step. The software component files were corrupted during the transfer to the IBM 6611. You can attempt to recover by applying the software component directly from the diskette or resending it.

If the installation of the new component fails after the previous component has been saved, the previous component is reinstated automatically. If this fails, you are probably in a broken state. Call your IBM service personnel for assistance.

If after running the new component, you decide that you would rather use the previous one, you can reinstate the previous component.

When the previous component is reinstated, either automatically or manually, the software vital product data is updated to show the reinstated software component as the one installed, and it shows all of its updates as committed. There is no record of the attempt to install the new component.

If after running the new component, you decide that you never need to reinstate the previous component that was saved, you can remove the saved component. This saves about 16 MB of space where the saved software files are stored.

When installing software components from the transfer directory, the software component images are removed from the directory after installation.

Restarting System after Software Installation

After a new version of software, either an update or a component, has been installed, that version becomes the current version whether or not it has been applied or committed.

Warning: Immediately after the installation of software changes, the IBM 6611 must be restarted.

The Software Installation and Maintenance Facility provides a system restart command for this purpose. If one of the peer-capable adapters is in a disabled state before the system is restarted, it will remain disabled after the system is restarted. Any new adapter code destined for that adapter is not downloaded in that situation. The IBM 6611 should be powered off and back on again after a minute to start the adapter and to cause the new code to be downloaded to the adapter.

Software Installation Procedure

To perform software installation from the System Manager,

1. Log in to the System Manager using a controlling userid. See "Userids and Passwords" on page 9-25 for information about controlling userids.
2. Select **Software Installation and Maintenance** on the main menu.

Figure 12-1 on page 12-7 displays the Software Installation and Maintenance menu.

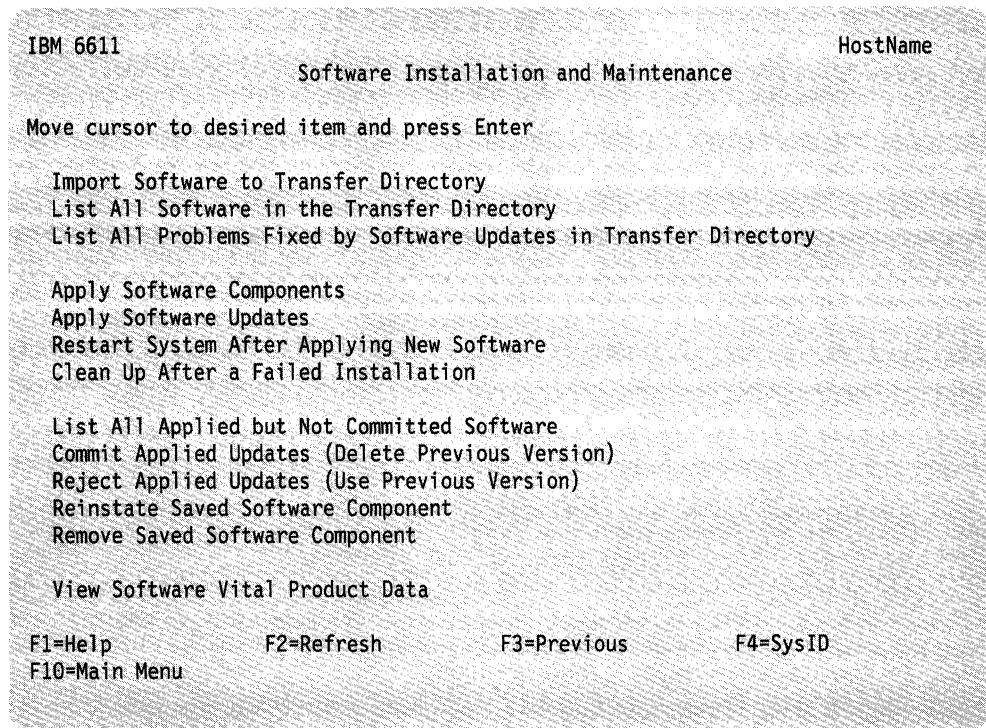


Figure 12-1. Software Installation and Maintenance Menu

Follow this procedure to install your software installation package using the System Manager:

Step 1 Your software installation package is sent to you on diskettes. It can contain software updates, software components, or both. The software package can be installed either from the diskettes or from the transfer directory. To install the software package from the diskettes, you should be in close proximity to the IBM 6611 in order to insert the diskettes when requested. Go to **Step 5**, if you are installing the software from the diskettes.

Step 2 Select **Import Software to Transfer Directory** to transfer the installation files to the transfer directory in the IBM 6611. Three import methods are available:

- FTP
- Modem
- Diskette.

Before you transfer the software changes to the transfer directory, ensure that there is enough space in the directory for the software images. The software package should state how much space is needed. To find out how much space is available in the transfer directory using the System Manager:

1. Select **System Environment and Configuration** from the main System Manager menu.
2. Select **Work with Files in Transfer Directory** from the next menu.
3. Select **View** from the selector screen.

You receive a screen that lists the files in the transfer directory. At the top of the screen you can find the free space available in the transfer directory. If the transfer directory does not have enough space, you need to delete all

unnecessary files from that directory. See “Working with Files in the Transfer Directory” on page 10-19 for information about deleting files in the transfer directory.

See “Transferring Software Changes to an IBM 6611” on page 12-25 for more information about importing the software files.

Press **F3 (Esc + 3)** until you return to the main Software Installation and Maintenance menu.

Step 3 To view a list of the software in the transfer directory of the IBM 6611, select **List All Software in the Transfer Directory** to list the software. Sample output from this command is shown in Figure 12-2.

Option Name	Level	I/U Q Content
mpnp.obj	01.01.0000.0003.NP61003	U Y usr,root
# Multiprotocol Network Program		
mpnp.obj	01.01.0000.0002.NP61002	U Y usr,root
# Multiprotocol Network Program		
mpnp.obj	01.01.0000.0001.NP61001	U Y usr,root
# Multiprotocol Network Program		

Figure 12-2. Sample List of Software in Transfer Directory

Press **F3 (Esc + 3)** until you return to the main Software Installation and Maintenance menu.

Go to **Step 6** if you are installing only software components.

Step 4 To view the list and select from the list:

1. Select **List All Problems Fixed by Software Updates in Transfer Directory** to list the problems fixed by the software updates in the transfer directory.
2. Press **F9 (Esc + 9)** to select the update name on the selector screen that follows. There are two methods for selecting the update name. Select one of the following:

mpnp.all List the problems fixed by **all** the software updates in the transfer directory.

Any number of the listed updates

List the problems fixed by the selected software updates in the transfer directory.

Software updates are in the form:

mpnp.obj.01.01.0000.0000.NP12345
mpnp.data.01.01.0000.0000.NP12345

Press **Enter** to record the selections.

Sample output from this command is shown in Figure 12-3.

Fix information

files restored: 2

usr/share fix information for
mpnp.obj 1.1.00.003.NP61003
NP61003 Test software update3

Required 1.1 update.

root fix information for
mpnp.obj 1.1.00.003.NP61003
NP61003 Test software update3

Required 1.1 update.

files restored: 2

usr/share fix information for
mpnp.obj 1.1.00.002.NP61002
NP61002 Test software update2

Required 1.1 update.

root fix information for
mpnp.obj 1.1.00.002.NP61002.
NP61002 Test software update2

Required 1.1 update.

files restored: 2

usr/share fix information for
mpnp.obj 1.1.00.001.NP61001
NP61001 Test software update1

Required 1.1 update.

root fix information for
mpnp.obj 1.1.00.001.NP61001
NP61001 Test software update1
Required 1.1 update.

Figure 12-3. Sample List of Problems Fixed by Software Updates

Press **F3 (Esc + 3)** until you return to the main Software Installation and Maintenance menu.

Step 5 This step installs the software updates in the package.

1. Select **Apply Software Updates** to install the software updates in the package.

2. On the selector screen that follows, select:

transfer_directory

If the software updates are in the transfer directory of this IBM 6611

diskette

If the software updates are in the diskette drive of the IBM 6611.

3. On the next selector screen, choose whether or not you want to automatically restart the IBM 6611 after a successful installation. Select:

yes The system will be automatically restarted if the installation is successful.

no The system will not be automatically restarted if the installation is successful. Issue **Restart the System after Software Installation** after the installation is complete, if you choose this option.

4. Press **F9 (Esc + 9)** to select **Update names** on the selector screen that follows. There are two methods for selecting the update name. Select one of the following:

mpnp.all

Apply **all** the software updates.

Any number of the listed updates

Apply each of the selected software updates.

Software updates are in the form:

mpnp.obj.01.01.0000.0000.NP12345

mpnp.data.01.01.0000.0000.NP12345

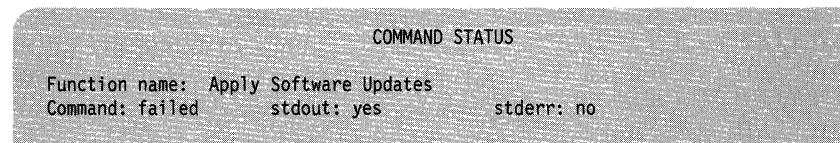
Press **Enter** to record the selections.

If you are applying the software updates from diskettes and the installation command is suspended, press **Ctrl + C** if you want to end the suspension. If the installation is suspended, the bottom of the dialog screen will have the *Processing data ...* message as shown below.



Press **Ctrl + C** if you want to end this operation.

If you receive error messages during the software installation, the installation may have failed. If there is an error in the installation, the following message appears at the top of the COMMAND STATUS screen:



It may be necessary to scroll the installation output on this screen to find the installation error messages. If failures are detected or if the installation process is interrupted, the Software Installation and Maintenance Facility attempts to “clean up” by removing software updates that were partially installed and restoring the component to its state before attempting to install the software update. If the system successfully returns to the previous state, that version of the component becomes the current version. If this cannot be done, the software component is marked as broken. IBM recommends that you reinstate any broken software components.

In most cases the Software Installation and Maintenance Facility’s automatic cleanup is successful. Normally, the only situation when a manual cleanup needs to be performed is when the system shuts down or loses power during the installation. If you have a problem with your installation that results in a partial installation and the automatic “cleanup” is not successful, select **Clean Up After a Failed Installation** to clean up the partial installation and restore the saved file.

The installation of software updates can fail for several reasons:

1. There is insufficient space in the file system where the saved files are stored, when the update is applied. To create more space, you can:
 - Commit applied software updates. See “Commit Applied Updates (Delete Previous Version)” on page 12-16 for details.
 - Remove the saved software component. See “Remove Saved Software Component” on page 12-18 for details.
2. The software update failed its verification during the install step. The software update files were corrupted during the transfer to the IBM 6611. You can attempt to recover by applying the software updates directly from the diskette or resending them.
3. Software updates that are a prerequisite to the one being applied have not already been applied and are not part of the software package being applied. Software updates that are a corequisite to the one being applied are not part of the software package being applied. Make sure all updates that have dependencies on other updates are applied at the same time.

A summary report is provided at the end of the installation step that lists the status of each of the software updates that have been installed. Figure 12-4 is an example of the summary report generated after installation of some Multiprotocol Network Program updates.

Install Summary

Name	Fix Id	Part	Event	Result	State
mpnp.obj	NP61003	USR	APPLY	SUCCESS	APPLIED
mpnp.obj	NP61003	ROOT	APPLY	SUCCESS	APPLIED
mpnp.obj	NP61002	USR	APPLY	SUCCESS	APPLIED
mpnp.obj	NP61002	ROOT	APPLY	SUCCESS	APPLIED
mpnp.obj	NP61001	USR	APPLY	SUCCESS	APPLIED
mpnp.obj	NP61001	ROOT	APPLY	SUCCESS	APPLIED

Figure 12-4. Software Update Installation Output

Press **F3 (Esc + 3)** until you return to the main Software Installation and Maintenance menu.

Go to **Step 7** if you do not have any software components to install.

Step 6 This step installs the software components in the package. A software component, when installed, overlays the previous software component by the same name. The previous component and all its installed updates are saved.

All uncommitted software updates for the previous software component must be either committed or rejected before the installation of the new software component. If this is not done, you receive an error message when you attempt to install the new component. See "Commit Applied Updates (Delete Previous Version)" on page 12-16 for details on committing updates. See "Reject Applied Updates (Use Previous Version)" on page 12-17 for details on rejecting updates.

1. Select **Apply Software Components** to install the software components in the package.

2. On the selector screen that follows, select:

transfer_directory If the software components are in the transfer directory of this IBM 6611

diskette If the software components are in the diskette drive of the IBM 6611.

3. On the next selector screen, choose whether or not you want to automatically restart the IBM 6611 after a successful installation. Select:

yes The system will be automatically restarted if the installation is successful.

no The system will not be automatically restarted if the installation is successful. Issue **Restart the System after Software Installation** after the installation is complete, if you choose this option.

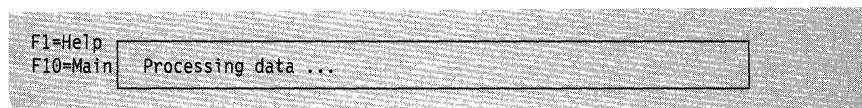
4. Press **F9 (Esc + 9)** to select the **Component name** on the selector screen that follows. There are two methods for selecting the component name. Select one of the following:

mpnp.all
Apply **all** the software components.

mpnp.obj or mpnp.data
Apply each of the selected software components.

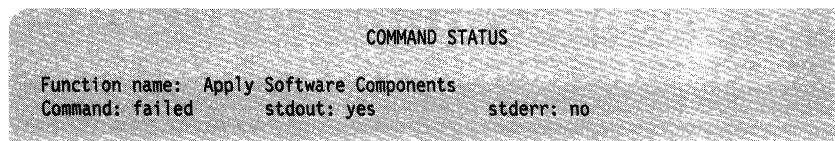
Press **Enter** to record the selections.

If you are applying the software components from diskettes and the installation command is suspended, press **Ctrl + C** if you want to end the suspension. If the installation is suspended, the bottom of the dialog screen will have the *Processing data ...* message as shown below.



A possible cause for the problem is the wrong diskette is in the diskette drive or there is no diskette in the diskette drive.

If you receive error messages during the software installation, the installation may have failed. If there is an error in the installation, the following appears at the top of the COMMAND STATUS screen:



It may be necessary to scroll the installation output on this screen to find the installation error messages.

The installation of software components can fail for several reasons:

1. There is insufficient space in the file system where the saved component is stored, when the new component is applied. When this occurs, you are asked whether or not you want to continue with the component installation without saving the component being overlaid. If you choose to abruptly end the installation, you can create more space to save the software component being overlaid by committing applied software updates. See "Commit Applied Updates (Delete Previous Version)" on page 12-16 for details about committing updates.
2. The software component failed its verification during the install step. The software component files were corrupted during the transfer to the IBM 6611. You can attempt to recover by applying the software component directly from the diskette or resending it.

If the installation of the new component fails after the previous component has been saved, the previous component is reinstated automatically. If this fails, you are probably in a broken state. Please call your service representative for help.

A summary report is provided at the end of the installation step that lists the status of each of the software components that were installed.

Figure 12-5 is an example of the summary report generated after installation of the Multiprotocol Network Program software components.

Install Summary

Name	Fix Id	Part	Event	Result	State
mpnp.obj		USR	APPLY	SUCCESS	COMMITTED
mpnp.obj		ROOT	APPLY	SUCCESS	COMMITTED
mpnp.data		SHARE	APPLY	SUCCESS	COMMITTED

Figure 12-5. Software Component Installation Output

Press **F3 (Esc + 3)** until you return to the main Software Installation and Maintenance menu.

Step 7 After a new version of software, an update or a component, has been installed, that version becomes the current version (whether or not it has been applied or committed).

Warning: Immediately after the installation of software changes, the IBM 6611 must be restarted.

It is important to schedule the installation of software changes at a time of low usage for the IBM 6611.

There is a command to stop and restart the IBM 6611. This command stops all operations in the base operating system, including all routing needing to access the main system and all user sessions. This command does not stop the operation of the peer-capable adapters, unless they are attempting to communicate to the main operating system.

If one of the peer-capable adapters is in a disabled state before the system is restarted, it will remain disabled after the system is restarted. Any new adapter code destined for that adapter is not downloaded in that situation. The IBM 6611 should be powered off and back on again after a minute to restart the adapter and to cause the new code to be downloaded to the adapter.

Before the beginning of the system restart, users are notified with a message stating the number of minutes before the system will be shut down. There are a series of messages that are displayed during the shutdown process. These messages vary slightly depending on whether you are connected over an EIA 232 serial port or a remote network connection, such as TELNET. See Figure 12-6 for an example of the system restart messages received over a direct connection. The last line is not displayed, if the system restart is issued from a remote user over a TELNET session.

SHUTDOWN PROGRAM

Sun Dec 22 18:07:50 1991

Broadcast message from ibm6611c on tty ...

PLEASE LOG OFF NOW !!!

System maintenance in progress.
All processes will be killed in 3 minutes.

Broadcast message from ibm6611c on tty ...

THE SYSTEM IS BEING BROUGHT DOWN NOW

Process accounting has stopped.
Error reporting has stopped.
Stopping NFS/NIS Daemons
The Subsystem or Group, nfsd, is currently inoperative.
The Subsystem or Group, biod, is currently inoperative.
The Subsystem or Group, rpc.lockd, currently inoperative.
The Subsystem or Group, rpc.statd, currently inoperative.
The Subsystem or Group, rpc.mountd, currently inoperative.
The Subsystem or Group, yppasswdd, currently inoperative.
The Subsystem or Group, ypupdated, currently inoperative.
All processes currently running will now be killed.

Figure 12-6. System Restart Messages

To restart the IBM 6611 after applying software changes using the System Manager:

1. Select **Restart System After Applying New Software**.
2. A dialog screen is displayed. Enter the elapsed time, in minutes, when the system begins to shut down.
3. You will receive the following two messages warning you of the results of shutting down your IBM 6611:

ARE YOU SURE?

Executing this command will shut down your IBM 6611, stopping all the protocols and processes including the current System Manager session.
Press Enter to shutdown the IBM 6611.
Press Previous to cancel and return to the System Manager.

F1=Help F2=Refresh F3=Previous
F10=Main Menu

INFORMATION MESSAGE

NOTE: This command needs to be run outside of the System Manager. Therefore the System Manager will exit immediately before running this command.

Press Enter to proceed with the command.

Press Previous to cancel and return to the System Manager.

F1=Help F2=Refresh F3=Previous
F10=Main Menu

To continue with the system restart, press **Enter** twice.

If you were logged in to the IBM 6611 through a direct-attached terminal, the login screen will appear when the system has been restarted. At that point you can log back in to the IBM 6611.

If you were logged into the IBM 6611 through a TELNET session, wait for a while before attempting to log back in. The connection will be refused until the system has been restarted.

Post Software Installation Functions

There are several software installation-related functions that may need to be performed after the software has been installed. The following sections explain how and when to perform these functions:

- Clean Up After a Failed Installation
- Commit Applied Updates (Delete Previous Version)
- Reject Applied Updates (Use Previous Version)
- Reinstate Saved Software Component
- Remove Saved Software Component.

Clean Up After a Failed Installation

During the installation process, status and error messages are written to the terminal. If the installation fails, an indication of why should be displayed on the terminal. If failures are detected or, if the installation process is interrupted, the Software Installation and Maintenance Facility attempts to “clean up” by removing software updates that were partially installed and restoring the component to its state prior to attempting to install the software update.

In most cases the Software Installation and Maintenance Facility's automatic cleanup is successful. Normally, the only scenario when you must perform a manual cleanup is when the system shuts down or loses power during the installation. If you have a problem with your installation that results in a partial installation and the automatic “cleanup” is not successful, select **Clean Up After a Failed Installation** to clean up the partial installation and restore the saved file.

A command status is displayed reporting the success or failure of the manual cleanup attempt.

If the system successfully returns to the previous state, that version of the component becomes the current version. If this cannot be done, the software component is marked as broken. IBM recommends that you reinstate any broken software components.

Commit Applied Updates (Delete Previous Version)

After running a new applied software update, you can decide to commit the update as permanent or to reject the update and use the previously saved files. The commit and reject functions are valid only for software updates that are applied, and not committed.

Committing software updates removes the files that were saved when the update was applied. This frees space so that other software updates or components can be applied.

Warning: When you **commit** the software update, the change is permanent.

Before committing a software update:

- Determine all the updates that are a prerequisite to the update you are committing. Select **List Prerequisites of a Software Component** on the **View Software Vital Product Data** menu for that determination. See “List Prerequisites of a Software Component” on page 12-36. If an update is a prerequisite to the one being committed, it also will be committed, if not already committed. Select **List All Applied but Not Committed Software** to list all the software that has been applied, but not committed. Press **Enter** to view the list. See Figure 12-7 on page 12-17 for an example of this list.

- Evaluate the effect of the update and its uncommitted prerequisites on your system's performance.

Name	Part	Level	State

mpnp.obj	USR	01.01.0000.0003.NP61003	APPLIED
mpnp.obj	ROOT	01.01.0000.0003.NP61003	APPLIED
mpnp.obj	USR	01.01.0000.0002.NP61002	APPLIED
mpnp.obj	ROOT	01.01.0000.0002.NP61002	APPLIED
mpnp.obj	USR	01.01.0000.0001.NP61001	APPLIED
mpnp.obj	ROOT	01.01.0000.0001.NP61001	APPLIED

Figure 12-7. List of Applied But Not Committed Software Example

If after careful examination of the situation, you decide to commit the software update:

1. Select **Commit Applied Updates (Delete Previous Version)**.
2. Press **F9 (Esc + 9)** to select the update name on the selector screen that follows. There are two methods for selecting the update name. Select one of the following:

mpnp.all

Commit **all** the software updates that are applied.

Any number of the listed updates

Commit each of the selected software updates.

Software updates are in the form:

mpnp.obj.01.01.0000.0000.NP12345

mpnp.data.01.01.0000.0000.NP12345

Press **Enter** to record the selections.

Reject Applied Updates (Use Previous Version)

After running a new applied software update, you can decide to commit the update as permanent or to reject the update and use the previously saved files. The commit and reject functions are valid only for software updates that are applied but not committed.

Rejecting software updates removes the update files from the current system and replaces them with the files that were saved when the update was applied. This frees space so that other software updates can be applied.

Before rejecting a software update:

- Determine all the updates that are dependents of the update you are rejecting. Select **List Dependents of a Software Component** on the **View Software Vital Product Data** menu for that determination. See "List Dependents of a Software Component" on page 12-37. If an update is a dependent of the one being rejected, it also will be rejected. Select **List All Applied but Not Committed Software** to list all the software that has been applied but not committed. Press **Enter** to view the list. See Figure 12-7 for an example of this list.
- Evaluate the effect of rejecting the update and its dependents on your system's performance.

If after careful examination of the situation, you decide to reject the software update:

1. Select **Reject Applied Updates (Use Previous Version)**.
2. Press **F9 (Esc + 9)** to select the update name on the selector screen that follows. There are two methods for selecting the update name. Select one of the following:

mpnp.all

Reject **all** the software updates that are applied.

Any number of the listed updates

Reject each of the selected software updates.

Software updates are in the form:

mpnp.obj.01.01.0000.0000.NP12345
mpnp.data.01.01.0000.0000.NP12345

Press **Enter** to record the selections.

Reinstate Saved Software Component

If after running a new software component, you decide that you rather run the previous component, you can reinstate the previous component. When the previous component is reinstated, the software vital product data is updated to show the reinstated software component as the one installed, and it shows all of its updates as committed. There is no record of the attempt to install the new component.

Select **Reinstate Saved Software Component** to reinstate the previously saved software component.

On the selector screen, choose whether or not you want to automatically restart the IBM 6611 after the previous component is successfully reinstated. Select:

- yes** The system will be automatically restarted if the installation is successful.
- no** The system will not be automatically restarted, if the installation is successful. Please issue **Restart the System after Software Installation** after the software component is reinstated, if you choose this option.

When the mpnp components were saved during the installation of the new mpnp components, both mpnp.obj and mpnp.data were saved at the same time. When you decide to reinstate the saved components, both are reinstated in the same step.

Remove Saved Software Component

If after running the new component, you decide that you never need to reinstate the previous component that was saved when the new component was installed, you can removed the saved component. This saves about 16 MB of space in the system where the saved software files are stored.

Select **Remove Saved Software Component** to remove the saved component. When the mpnp components were saved during the installation of the new mpnp components, both mpnp.obj and mpnp.data were saved at the same time. When you decide to remove the saved components, both are removed in the same step.

Automating Software Installation and Maintenance Facility Functions

Software installation can be managed from any RISC System/6000 workstation, such as the IBM AIX NetView/6000 network management workstation. The software changes can be copied from the diskettes to a directory on the management station. From there FTP can be used to transfer the software to the IBM 6611. After the software is on the IBM 6611, you have two options to install the changes:

- Use TELNET to access the IBM 6611 and use the System Manager or the fast-path command primitives to install the software.
- Use **rexec** or **rsh** commands to install the software, either by issuing single commands or by issuing multiple command primitives included in RSH scripts.

The noninteractive **ftp** command and the **rsh** command primitives can be combined into scripts that automate the software installation process. Several primitives can install software components and updates. There are additional primitives to commit, reject, remove, reinstate, and verify the software and to list the software and its vital product data. For more information about these command primitives, see "Install Command Primitives" on page 8-62. The noninteractive **ftp** command has the following format:

```
ftp -c userid password action filename filetype hostname
```

Where:

userid the userid at the node to which the **ftp** command is sent

password the password of the userid at the node to which the **ftp** command is sent

action the transferring action:

- *get*
 - Retrieve a file from the node to which the **ftp** command is sent
- *put*
 - Send a file to the node to which the **ftp** command is sent

filename The filename or filename group of the file(s) being sent or received.

filetype Specify either *ascii* or *binary*

hostname The host name of the node to which the **ftp** command is sent.

Sending Software Updates to One IBM 6611

See Figure 12-8 on page 12-20 for an example of an FTP and RSH script that transfers all the software updates from a directory at the remote workstation and applies the software updates to the IBM 6611 specified in the script. The details of this script are explained in the script header. This script must be run at a RISC System/6000 workstation. It automates the software installation of one IBM 6611, but it could be duplicated for each IBM 6611 in your IP network.

```

# IBM Multiprotocol Network Program
# Script: apply_updt.6611host
#
# This shell script uses FTP to automatically send all the software
# updates (PTFs) from a specified directory on a remote workstation
# to the IBM 6611. The software updates are applied to the IBM 6611
# after they arrive.
#
# DEPENDENCIES: This script is run from a remote workstation that
#               contains the software updates (PTFs). All the
#               software updates that you want to apply must be in
#               the directory that you specify when you run this
#               script. It is advisable to just have software
#               updates in that directory.
#
# INPUT: The only input parameter is the name of the directory at
#        remote workstation where the software updates (PTFs) exist.
#
# COMMAND SYNTAX:  apply_updt.6611host <directory>
#
#       where apply_updt.6611host is the name of this script
#       <directory> is the name of the directory on the remote
#       workstation where the PTFs exist.
#       <directory> should be specified in full path form.
#       For example: /usr
#
#       The script has hard coded some variables that need to be changed
#       to fit your environment.
#
#       IBM 6611 variables:
#       6611host: host name for the IBM 6611
#       ibm6611c: controlling userid at the IBM 6611
#       ibm6611p: password of the controlling userid at the IBM 6611
#       Remote Workstation variables:
#       netman  : host name at the remote workstation
#       user    : user ID at the remote workstation
#       passwd  : password of the user ID at the remote workstation
#
# OUTPUT: The message output from this script and the installation
#         summary report and any installation error messages are
#         displayed on the console of the remote workstation where
#         this script is executed.
#
for i in `ls "$1"`
do
    rsh 6611host -l ibm6611c ibm6611c ftp -c user passwd get "$1"/"$i" bin netman
    if [ "$?" -ne 0 ]
    then
        echo The transfer of "$i" to the IBM 6611 was not successful.
        exit 1
    else
        echo "The transfer of the software update, $i, to 6611host was successful."
    fi
done

echo "The software updates are now being installed ..."

rsh 6611host -l ibm6611c ibm6611c install_upd all

if [ "$?" -eq 0 ]
then
    echo The software updates were successfully applied.
    exit 0
else
    echo The software updates failed to be applied.
    exit 1
fi

```

Figure 12-8. A Sample Script That Applies All Software Updates

This script is called `apply_updt.6611host`. It is shipped in the static directory of each IBM 6611. There is also a script information file shipped with it called `apply_updt.6611host.README`. If you want to use this script, you can send the files using the **ftp** command to your remote workstation and modify it to your needs.

Select the **Send Files to Another Node** menu item on the Remote Accesses to Other Nodes menu to do this. See “Exporting Files to a Remote Node” on page 10-52 for more details.

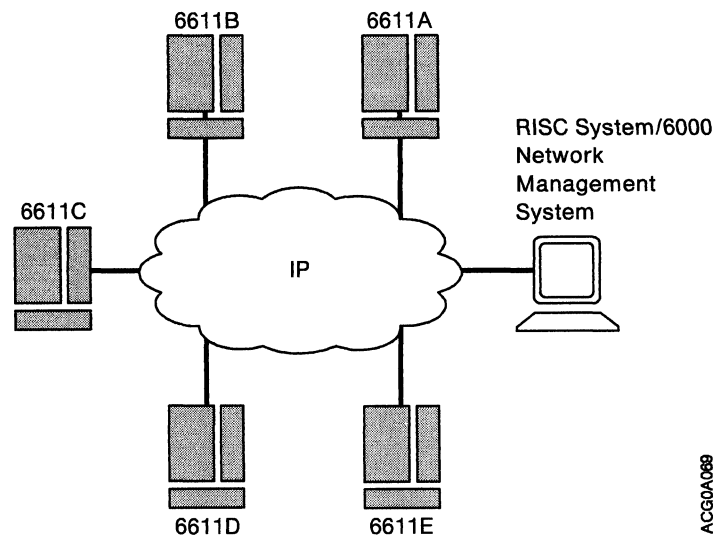


Figure 12-9. A Sample Configuration for Installing Software

Sending Software Updates to Multiple IBM 6611s

There is a script that automates the distribution and installation of software updates to multiple IBM 6611s. The script is named `apply_updt` and is located in the static directory of the IBM 6611. There is also an information file named `apply_updt.README` that contains instructions on executing the script. You may distribute and install updates across a single IP network or different IP networks provided there are routes between the networks.

The `apply_updt` script must be executed from a RISC System/6000 workstation and not the static directory of the IBM 6611. Send `apply_updt` to a RISC System/6000 workstation using FTP. At the workstation, create the necessary input file, `apply_updt.in`, containing the software update file names and the necessary information about each of the IBM 6611s requiring the software installation.

Warning: The length of time needed to add the new software component depends on the size of the software update.

The procedure for using this script is explained below:

- Step 1** The software installation package is sent to you on diskettes. Transfer the software files to a directory on the workstation. See “Transferring Software from Diskette to the RISC System/6000 Workstation” on page 12-27 for details.
- Step 2** Transfer the `apply_updt` script and the `apply_updt.README` file from the static directory of a IBM 6611 to the workstation. Select **Send Files to Another Node** on the Remote Accesses to Other Nodes menu to send the files via `ftp`. See “Exporting Files to a Remote Node” on page 10-52 for more details.

Step 3 Create the input file that is to be accessed by this script. The file name is `apply_updt.in`. The file should be stored in the same directory on the remote workstation where this script exists and from where this script is to be executed.

The input file, `apply_updt.in`, has the following format:

```
node:  nodename  ID  password  IPaddress
node:  nodename  ID  password  IPaddress
.
.
.
PTF:  full pathname of mpnp.obj update image
PTF:  full pathname of mpnp.data update image
```

Where

node A tag identifying this input statement as one describing an IBM 6611 to which the updates are to be applied.

nodename The host name or IP address of the IBM 6611 described in this statement.

ID A controlling userid for the IBM 6611 described in this statement.

password The password for the controlling userid.

IPaddress The IP address of the remote workstation from which this script is executed.

Note: This address is the workstation's address **not** the host's address.

PTF A tag identifying this input statement as one describing the full path and file name of the software update to be applied.

A sample `apply_updt.in` input file is shown in Figure 12-10. See Figure 12-9 on page 12-21 for a picture of the IP network.

```
node: 6611A 6611AC 6611AC 9.66.11.01
node: 6611B 6611BC 6611BC 9.66.11.01
node: 6611C 6611CC 6611CC 9.66.11.01
node: 6611D 6611DC 6611DC 9.66.11.01
node: 6611E 6611EC 6611EC 9.66.11.01
PTF: /usr/mpnp.obj.01.01.0000.0001.NP61001
PTF: /usr/mpnp.obj.01.01.0000.0002.NP61002
PTF: /usr/mpnp.obj.01.01.0000.0003.NP61003
```

Figure 12-10. Example `apply_updt.in` Input File

Step 4 Execute the `apply_updt` script. You are prompted for the password of the userid at the workstation from which you execute this script.

Step 5 The message output from this script is displayed on the screen of the workstation. This same output is also sent to the file `apply_updt.out`. The output file logs the status of the software changes that were made.

Figure 12-11 on page 12-23 shows an example of an output file created at the workstation after adding three software updates to multiple IBM 6611s.

```
Starting to work on 6611A
Successfully transferred /usr/mpnp.obj.01.01.0000.0001.NP61001 to 6611A
Successfully transferred /usr/mpnp.obj.01.01.0000.0002.NP61002 to 6611A
Successfully transferred /usr/mpnp.obj.01.01.0000.0003.NP61003 to 6611A
Starting to work on 6611B
Successfully transferred /usr/mpnp.obj.01.01.0000.0001.NP61001 to 6611B
Successfully transferred /usr/mpnp.obj.01.01.0000.0002.NP61002 to 6611B
Successfully transferred /usr/mpnp.obj.01.01.0000.0003.NP61003 to 6611B
Starting to work on 6611C
Successfully transferred /usr/mpnp.obj.01.01.0000.0001.NP61001 to 6611C
Successfully transferred /usr/mpnp.obj.01.01.0000.0002.NP61002 to 6611C
Successfully transferred /usr/mpnp.obj.01.01.0000.0003.NP61003 to 6611C
Starting to work on 6611D
Successfully transferred /usr/mpnp.obj.01.01.0000.0001.NP61001 to 6611D
Successfully transferred /usr/mpnp.obj.01.01.0000.0002.NP61002 to 6611D
Successfully transferred /usr/mpnp.obj.01.01.0000.0003.NP61003 to 6611D
Starting to work on 6611E
Successfully transferred /usr/mpnp.obj.01.01.0000.0001.NP61001 to 6611E
Successfully transferred /usr/mpnp.obj.01.01.0000.0002.NP61002 to 6611E
Successfully transferred /usr/mpnp.obj.01.01.0000.0003.NP61003 to 6611E
```

Figure 12-11. Example of the apply_updt.out File

Sending Software Components to Multiple IBM 6611s

There is a script that automates the distribution and installation of software components to multiple IBM 6611s. The script is named `apply_comp` and is located in the static directory of the IBM 6611. There is also an information file named `apply_comp.README` that contains instructions about executing the script. You may distribute and install components across a single IP network or different IP networks provided there are routes between the networks.

The `apply_comp` script must be executed from a RISC System/6000 workstation and not the static directory on the IBM 6611. Transfer `apply_comp` to a RISC System/6000 workstation using FTP. At the workstation, create the necessary input file, `apply_comp.in`, containing the software component file names and the necessary information about each of the IBM 6611s requiring the software installation.

Warning: The length of time needed to add the new software component depends on the size of the software component. One component takes approximately 30 minutes to send and install. Each additional 6611 that you want to install will increase the number of minutes by approximately 5 minutes.

The procedure for using this script is explained below:

- Step 1** The software installation package is sent to you on diskettes. Transfer the software files to a directory on the workstation. See “Transferring Software from Diskette to the RISC System/6000 Workstation” on page 12-27 for details.
- Step 2** Transfer the `apply_comp` script and the `apply_comp.README` file from the static directory of a IBM 6611 to the workstation. Select the **Send Files to Another Node** menu item on the Remote Accesses to Other Nodes menu to send the files using **ftp**. See “Exporting Files to a Remote Node” on page 10-52 for more details.

Step 3 Create the input file that is to be accessed by this script. The file name is `apply_comp.in` and should be stored in the same directory on the remote workstation where this script exists and where this script is to be executed.

The input file, `apply_comp.in`, has the following format:

```
node: nodename ID password IPaddress
node: nodename ID password IPaddress
.
.
.
file: full pathname of mpnp.obj image
file: full pathname of mpnp.data image
```

Where:

node A tag identifying this input statement as one describing an IBM 6611 to which the components are to be applied.

nodename The host name or IP address of the IBM 6611 described in this statement.

ID A controlling userid for the IBM 6611 described in this statement.

password The password for the controlling userid.

IPaddress The IP address of the remote workstation from which this script is executed.

Note: This is the workstation's IP address **not** the IBM 6611's address.

file A tag identifying this input statement as one describing the full path and file name of the software component to be applied.

A sample input file, `apply_comp.in`, is shown in Figure 12-12. Figure 12-9 on page 12-21 shows an IP network using IBM 6611s.

```
node: 6611A 6611AC 6611AC 9.66.11.01
node: 6611B 6611BC 6611BC 9.66.11.01
node: 6611C 6611CC 6611CC 9.66.11.01
node: 6611D 6611DC 6611DC 9.66.11.01
node: 6611E 6611EC 6611EC 9.66.11.01
file: /usr/mpnp.obj.01.01.0001.0000
file: /usr/mpnp.data.01.01.0001.0000
```

Figure 12-12. Example `apply_comp.in` Input File

Step 4 Execute the **apply_comp** script. You are prompted for the password of the userid at the workstation from which you execute this script.

Step 5 The message output from this script is displayed on the screen of the workstation. This same output is also sent to the file `apply_comp.out`. There is also an `apply_comp_out` file located in the transfer directory of each IBM 6611 that was specified by a node statement in the `apply_comp.in` input file. The output file logs the status of the software changes that were made. Figure 12-13 on page 12-25 shows an example of an output file created at the workstation after adding a software component to multiple IBM 6611s. Figure 12-14 on page 12-25 shows an example of an output file created at one of the IBM 6611s after adding a software component to it.

```
Starting to work on 6611A
Successfully transferred /usr/mpnp.data.01.01.0001.0000 to 6611A.
Successfully transferred /usr/mpnp.obj.01.01.0001.0000 to 6611A.
Starting to work on 6611B
Successfully transferred /usr/mpnp.data.01.01.0001.0000 to 6611B.
Successfully transferred /usr/mpnp.obj.01.01.0001.0000 to 6611B.
Starting to work on 6611C
Successfully transferred /usr/mpnp.data.01.01.0001.0000 to 6611C.
Successfully transferred /usr/mpnp.obj.01.01.0001.0000 to 6611C.
Starting to work on 6611D
Successfully transferred /usr/mpnp.data.01.01.0001.0000 to 6611D.
Successfully transferred /usr/mpnp.obj.01.01.0001.0000 to 6611D.
Starting to work on 6611E
Successfully transferred /usr/mpnp.data.01.01.0001.0000 to 6611E.
Successfully transferred /usr/mpnp.obj.01.01.0001.0000 to 6611E.
```

Figure 12-13. Example of the apply_comp.out File

```
Current component is being saved.
The current component was saved SUCCESSFULLY.
The Table of Contents (.toc) file in the transfer directory is being updated.
The component located in the transfer directory is being installed.
The installation was SUCCESSFUL.
The component image was SUCCESSFULLY removed from the transfer directory.
The 6611 is being shutdown and restarted.
```

Figure 12-14. Example of the apply_comp_out File

Transferring Software Changes to an IBM 6611

Software changes are sent to you on a diskette. The software changes (components and updates) can be installed from the diskettes on which they arrive or from the transfer directory. There are four methods available to transfer the software changes to this directory:

Method A

Place the software diskettes in the diskette drive of the IBM 6611 needing the software change. Copy the files on the diskettes into the transfer directory. See "Transferring Software from a Diskette to an IBM 6611" on page 12-26 for information about importing files from a diskette.

Method B

1. Place the software diskettes in the diskette drive of another IBM 6611 on the same IP network as the IBM 6611 needing the software change. Copy the files on the diskettes into the transfer directory. See "Transferring Software from a Diskette to an IBM 6611" on page 12-26 for information about importing files from a diskette.
2. Use FTP to transfer the software changes to the transfer directory of the IBM 6611 needing the software change. Refer to "Transferring Software from an IBM 6611 to an IBM 6611 Using FTP" on page 12-30 for information about using FTP.

Method C

1. Place each of the software diskettes in the diskette drive of an RISC System/6000 workstation on the same IP network as the IBM 6611 needing the software change. Copy the files on the diskettes to a directory on the RISC System/6000 workstation. Refer to "Transferring Software from Diskette to the RISC System/6000 Workstation" on page 12-27 for information about importing files to a RISC System/6000 workstation.
2. Use FTP to transfer the software changes to the transfer directory in the IBM 6611. Refer to "Transferring Software from a RISC System/6000 Workstation to an IBM 6611 Using FTP" on page 12-28 for information about using FTP.

Method D

- Place each of the software diskettes in the diskette drive of an RISC System/6000 workstation that has call-out modem access to the public switch network. Copy them to a directory on the RISC System/6000 workstation. Refer to "Transferring Software from Diskette to the RISC System/6000 Workstation" on page 12-27 for information about importing files to a RISC System/6000 workstation.
- Establish a connection to a RISC System/6000 workstation or to an IBM 6611 on the same IP network as the IBM 6611 needing the software changes. Transfer the software to the transfer directory of the IBM 6611 using Xmodem. Refer to "Transferring Software from a RISC System/6000 Workstation to an IBM 6611 Using Xmodem" on page 12-32 for information about using Xmodem.

Transferring Software from a Diskette to an IBM 6611

The software changes are sent to you on a diskette or several diskettes depending on the size of the software installation package. You can decide to install the software package directly from the diskette or transfer them from the diskette into the transfer directory. If you decide to use the diskette drive of the IBM 6611, IBM recommends that you are located at a direct-attached or remote-attached terminal which is located close to the IBM 6611. Use the following scenario to place the software updates into the transfer directory of the IBM 6611 using the System Manager:

- Step 1** Place the software diskette in the diskette drive of the IBM 6611.
- Step 2** Select **Software Installation and Maintenance** from the main menu.
- Step 3** Select **Import Software to Transfer Directory** from the next menu.
- Step 4** Select **diskette** from the selector screen.
- Step 5** Select **mpnp.all** on the selector screen. This causes all the software to be transferred.
- Step 6** Follow any messages that appear requesting you to insert the next diskette, if more than one.

If the installation command becomes suspended, press **Ctrl + C** to end the suspension. The bottom of the dialog screen will have the *Processing data ...* message as shown below.

F1=Help
F10=Exit Processing data ...

A possible cause for the problem is the wrong diskette is in the diskette drive or there is no diskette in the diskette drive. Retry to import the software. You may need to delete the partially imported software from transfer directory and start again from the beginning.

Transferring Software from Diskette to the RISC System/6000 Workstation

If you want to perform your software installation tasks remotely from a central location, you can either import the software from a RISC System/6000 workstation or from another IBM 6611 and distribute the files using FTP. The remote stations must be on the same IP network as the IBM 6611 needing the software change. See "Transferring Software from a Diskette to an IBM 6611" on page 12-26, if you are using another IBM 6611. You can use the following scenario to copy the software diskettes to the */usr* directory of a RISC System/6000 workstation, that is used for remote installation. These instructions assume that the RISC System/6000 workstation is using AIX Version 3.2.

- Step 1** Place the software diskette in the diskette drive of the RISC System/6000 workstation on the same IP network as the IBM 6611 needing the software change.
- Step 2** Import the software from the diskettes to the directory */usr*, using either the System Management Interface Tool (SMIT) or using a command from the shell prompt:
- Using the System Management Interface Tool (SMIT):
 1. Select **Installation and Maintenance** from the main menu.
 2. Select **Standard Installation and Maintenance** from the next menu.
 3. Select **Software Installation and Maintenance** from the next menu.
 4. Select **Copy Software to Hard Disk for Future Installation** from the next menu.
 5. Press **F4 (Esc + 4)** to get a selection list for INPUT device/directory for software.
 6. Select **/dev/fd0** from the list and press **Enter**.
 7. Change the DIRECTORY for storing software from */usr/sys/inst.images* to */usr* and use the defaults for the other entry fields.
 8. Respond to any messages that appear requesting you to insert the next diskette, if there is more than one.
 - Using the command line:
 1. Enter the following command from the shell prompt on the RISC System/6000 workstation:
bffcreate -qv -d /dev/fd0 -t /usr -X all
 2. Follow any messages that appear requesting you to insert the next diskette, if more than one.

Transferring Software from a RISC System/6000 Workstation to an IBM 6611 Using FTP

The following scenario can be used to copy the software installation package from the RISC System/6000 workstation to the IBM 6611 needing the software change using FTP. This scenario assumes that you have previously copied the software installation package to the fixed disk of the */usr* directory of the RISC System/6000 workstation using "Transferring Software from Diskette to the RISC System/6000 Workstation" on page 12-27. The information you are expected to type in is provided under the heading, **Type In**. The information you should see displayed on the screen is provide under the heading, **Output displayed**.

Type in:

```
cd /usr
ftp hostname
```

The IP address of the IBM 6611 can be used in the place of the host name.

Output displayed:

```
Connected to hostname.
220 hostname FTP server (Version 4.1 Date) ready.
Name (hostname: risc_userid):
```

Type in:

```
6611_userid
```

Output displayed:

```
331 Password required for 6611_userid.
Password:
```

Type in:

(Enter the password. It will not be displayed.)

Output displayed:

```
230 User 6611_userid logged in.
/transfer is read-write and /static is read-only.
ftp>
```

Type in:

```
cd /transfer
```

Output displayed:

```
250 CWD command successful.
ftp>
```

Type in:

```
bi
```

Output displayed:

```
200 Type set to I.  
ftp>
```

Type in:

```
mput *
```

Output displayed:

Each file in the directory is displayed and you are given the opportunity to state whether or not you want to send it.

```
mput filename1?
```

Type in:

Type **y** for each file in the software installation package that you want to send to the IBM 6611. Type **n** for those files you do not want to send.

```
y
```

Output displayed:

```
200 PORT command successful.  
150 Opening BINARY mode data connection for filename1.  
226 Transfer complete.  
13029 bytes sent in 0.07388 seconds (172.2 Kbytes/s)  
mput filename2?
```

Type in:

```
y
```

Output displayed:

```
200 PORT command successful.  
150 Opening BINARY mode data connection for filename2.  
226 Transfer complete.  
13029 bytes sent in 0.07388 seconds (172.2 Kbytes/s)  
ftp>
```

Type in:

```
quit
```

Output displayed:

```
221 Goodbye.
```

Note: The numbers associated with the FTP messages are standard message numbers for this protocol. They have no significance other than to identify the message. See "Using the File Transfer Protocol" on page 10-52 for more information about FTP.

Transferring Software from an IBM 6611 to an IBM 6611 Using FTP

The following scenario can be used to copy the software placed in the transfer directory from one IBM 6611 to another IBM 6611 needing the software change using FTP. This scenario assumes that you have previously copied the software installation package into the transfer directory of the remote IBM 6611 using "Transferring Software from a Diskette to an IBM 6611" on page 12-26. This process uses the System Manager.

Step 1 Write down the names of the software changes that have previously been placed in the transfer directory of the remote IBM 6611:

- Select **Software Installation and Maintenance** on the main menu.
- Select **List All Software in the Transfer Directory** on the next menu.
- Write down the names of the software changes that you want to transfer to the IBM 6611 needing the software change, and any matching patterns in the names of the software changes. For example, the following two software subcomponents contain the pattern "mpnp".

```
mpnp.obj.01.01.0001.0000  
mpnp.data.01.01.0001.0000
```

- Press **F3 (Esc + 3)** until you reach the main menu of the System Manager.

Step 2 Transfer these files to the IBM 6611 needing the software changes using FTP.

1. Select **Remote Accesses to Other Nodes** on the main menu.
2. Select **Send Files to Another Node** on the next menu.
3. Select **FTP** as the transfer method from the selector screen.
4. Select **transfer directory** as the source of the files from the selector screen.
5. Type the host name or IP address of the IBM 6611 needing the software changes on the dialog item.
6. Press **Enter**. Use the following scenario should be used to transfer the software to the transfer directory of the IBM 6611 needing the software changes. The information you are expected to type in from the remote IBM 6611 is provided under the heading **Type in**. The output you should expect to see on the screen is provided under the heading **Output displayed**.

Type in:

(From the System Manager screen.)

ftp hostname

The IP address of the IBM 6611 can be used in the place of the host name.

Output displayed:

```
Connected to hostname.  
220 hostname FTP server (Version 4.1 Date) ready.  
Name (hostname: local_userid):
```

Type in:

```
6611_userid
```

Output displayed:

```
331 Password required for 6611_userid.  
Password:
```

Type in:

```
(Enter the password. It will not be displayed.)
```

Output displayed:

```
230 User 6611_userid logged in.  
/transfer is read-write and /static is read-only.  
ftp>
```

Type in:

```
cd /transfer
```

Output displayed:

```
250 CWD command successful.  
ftp>
```

Type in:

```
bi
```

Output displayed:

```
200 Type set to I.  
ftp>
```

Type in:

```
mput *pattern*
```

where *pattern* is "mpnp" in the example above.

Output displayed:

```
mput filename1?
```

Type in:

```
y
```

Output displayed:

```
200 PORT command successful.
150 Opening BINARY mode data connection for filename1.
226 Transfer complete.
13029 bytes sent in 0.07388 seconds (172.2 Kbytes/s)
```

Output displayed:

```
mput filename2?
```

Type in:

```
y
```

Output displayed:

```
200 PORT command successful.
150 Opening BINARY mode data connection for filename2.
226 Transfer complete.
53349 bytes sent in 0.09288 seconds (579.8 Kbytes/s)
ftp>
```

Type in:

```
quit
```

Output displayed:

```
221 Goodbye.
```

Transferring Software from a RISC System/6000 Workstation to an IBM 6611 Using Xmodem

The following scenario can be used to copy the software installation package from the */usr* directory of the RISC System/6000 workstation to the IBM 6611 needing the software change using Xmodem:

1. List the files in the */usr* directory and write down the file names. In this scenario, the file names are filename1, filename2
2. Establish a switched connection from the RISC System/6000 workstation containing the software images in the */usr* directory to any IBM 6611 that is attached to the public switched network through a modem connected to one of its EIA 232 serial ports. Refer to the RISC System/6000 documentation for information about using the Asynchronous Terminal Emulator (ATE) to perform this function.
3. Log in to the IBM 6611 and select the correct terminal type.
4. You are now in the IBM 6611's System Manager. From the System Manager, setup the IBM 6611 to receive the software:
 - Select **Software Installation and Maintenance** from main menu.
 - Select **Import Software to Transfer Directory** from next menu.
 - Select **modem** from the selector screen.
 - Type **filename1** for "Software to be imported" on the dialog screen.

You receive the following messages on the System Manager screen:

You can return to the local machine and begin the file transmission.
The system is ready to receive file filename1.
Use Ctrl+X to stop xmodem.

5. Press **Ctrl + V** at the RISC System/6000 workstation. Instruct the RISC System/6000 workstation to send the file by selecting **Send** or typing the following command on the command line of the Connected Main Menu:

s /usr/filename1

The software files are transferred to the transfer directory of the IBM 6611.

See "Using a Modem" on page 9-17 and "Transferring Files between a RISC System/6000 and IBM 6611" on page 10-55 for more details about using modems and transferring files between a RISC System/6000 workstation and an IBM 6611.

Saving Your Software and Configuration Diskettes

If the fixed disk fails, the IBM service personnel can order you a new fixed disk with the Multiprotocol Network Program already installed and replace your fixed disk. You are given information concerning the level of the software on the replacement fixed disk. You may be required to add software components or updates to restore the Multiprotocol Network Program to the level it was prior to the fixed disk failure. You should save copies of all your software installation packages to upgrade the fixed disk to the desired level quickly.

The new software on the IBM 6611 must be reconfigured. You should save copies of all your configuration changes on diskettes to quickly reconfigure the IBM 6611 after a fixed disk replacement.

Software Vital Product Data

The Software Installation and Maintenance Facility has the ability to maintain version control on all software currently located on the IBM 6611. This is done by maintaining a record in the vital product data (VPD) repository for each installable entity. The record layout is as follows:

UNIT NAME VV.RR.MMMM.FFFF

where:

UNIT NAME Describes the current installable entity

VV Version Level, such as 01

RR Release Level, such as 00

MMMM Modification Level.

This field is used only to track the installation of new software components. The MMMM is set to zero at the start of each new release and will be incremented with each new software component that is installed, until the next release is shipped.

FFFF Fix Level. This field serves as an identifier for software updates. It will be incremented for each software update produced for the component. Software updates will not be required to be installed in *fix level order* unless there is an identified prerequisite relationship that requires that order.

The facility maintains tables that contain information about all of the software updates that have been installed on the system. The database holds the status of the software changes (committed or applied), in addition to the prerequisite and corequisite information. You can query the information stored in this database using the System Manager, or the command primitives.

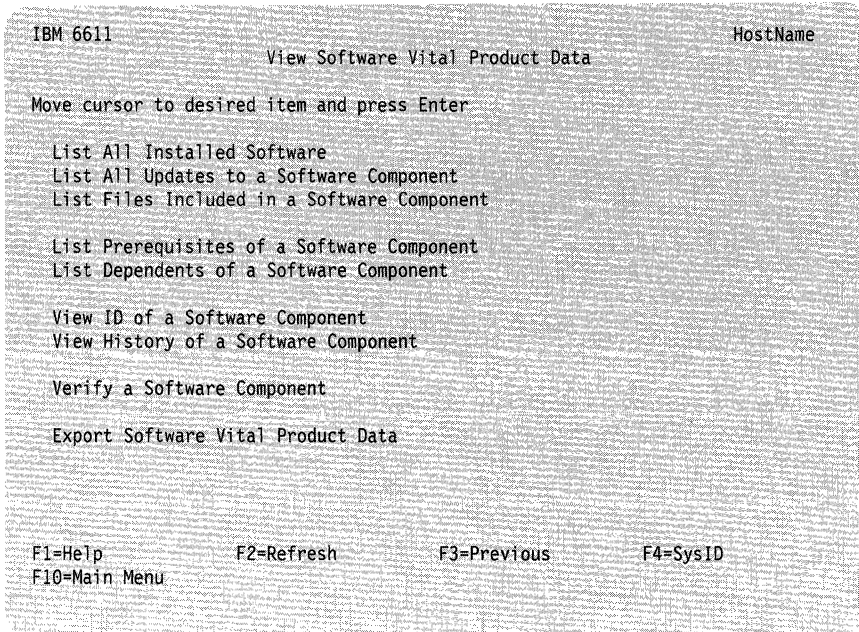


Figure 12-15. View Software Vital Product Data Menu

To query the software VPD from the System Manager, select **View Software Vital Product Data** on the Software Installation and Maintenance menu. Figure 12-15 shows the View Software Vital Product Data menu.

There are seven menu items associated with viewing information about installed software components and updates. You can have the output for each menu item sent to either the screen or the transfer directory. You can also verify a software component from this menu.

See these pages for more information about the individual menu items:

List All Installed Software	12-35
List All Updates to a Software Component	12-35
List Files Included in a Software Component	12-36
List Prerequisites of a Software Component	12-36
List Dependents of a Software Component	12-37
View ID of a Software Component	12-38
View History of a Software Component	12-38
Verify a Software Component	12-39
Exporting the Software Vital Product Data	12-40

List All Installed Software

To list all software components, select **List All Installed Software**.

The software components are listed along with their install state and a description of the component. Figure 12-16 is an example of the output received.

Name	State	Description
-----	-----	-----
Path: /usr/lib/objrepos		
mpnp.obj	COMMITTED	Multiprotocol Network Program
Path: /etc/objrepos		
mpnp.obj	COMMITTED	Multiprotocol Network Program
Path: /usr/share/lib/objrepos		
mpnp.data	COMMITTED	Multiprotocol Network Program

Figure 12-16. Sample List of All Installed Software

List All Updates to a Software Component

To list all the software updates installed on a selected software component:

1. Select **List All Updates to a Software Component**.
2. Press **F9 (Esc + 9)** to select each software component on the selector screen that follows. Press **Enter** to record the selections.
3. Press **Enter** to execute the function.

The software updates are listed along with their installed state, fix ID, and fix information. Figure 12-17 is an example showing software updates for the mpnp.obj component.

Name	Fix Id	State	Fix Information
-----	-----	-----	-----
Path: /usr/lib/objrepos			
mpnp.obj		COMMITTED	NONE
	R661001	APPLIED	NONE
	R661002	APPLIED	NONE
	R661003	APPLIED	NONE
Path: /etc/objrepos			
mpnp.obj		COMMITTED	NONE
	R661001	APPLIED	NONE
	R661002	APPLIED	NONE
	R661003	APPLIED	NONE
Path: /usr/share/lib/objrepos			
mpnp.data		COMMITTED	NONE

Figure 12-17. Sample List of All Updates to Software Components

List Files Included in a Software Component

To list all the files that are part of selected software components:

1. Select **List Files Included in a Software Component**.
2. Press **F9 (Esc + 9)** to select each software component on the selector screen that follows. Press **Enter** to record the selections.
3. Press **Enter** to execute the function.

All the files that are associated with the selected software components are listed. Figure 12-18 is an example showing a partial list of files for the mpnp.obj component.

Name	File
-----	-----
Path: /usr/lib/objrepos	
mpnp.obj	/tmp/etc
	/usr/lpp/mpnp/inst_root/etc/r66tools
	/usr/lpp/mpnp/inst_root/etc/ppp
	/usr/lpp/mpnp/inst_root/etc/usocktrc
	/usr/lpp/mpnp/inst_root/tmp/hold
	/usr/lpp/mpnp/inst_root/tmp/hold/static
	/usr/lpp/mpnp/inst_root/tmp/hold/transfer
	/usr/lib/ras
	/usr/lpp/diagnostics/da
	/usr/lpp/diagnostics/catalog/default
	/usr/lpp/diagnostics/catalog/En_US
	/usr/lib/methods
	/usr/lpp/diagnostics/bin
	/usr/sbin/tsm
	/usr/bin/tsh
	/usr/lpp/mpnp/inst_root/bin/udump
	/usr/lpp/mpnp/inst_root/bin/vutrc
	/usr/sbin/DNArouted
	/usr/sbin/XNSquery
	/usr/sbin/XNSrouted

Figure 12-18. Sample List of Files for Software Components

List Prerequisites of a Software Component

To list the prerequisites of selected software components:

1. Select **List Prerequisites of a Software Component**.
2. Press **F9 (Esc + 9)** to select each software component on the selector screen that follows. Press **Enter** to record the selections.
3. Press **Enter** to execute the function.

The selected software components are listed with their prerequisites. Figure 12-19 on page 12-37 is an example showing the prerequisites for the mpnp component.

Name	Prerequisites
Path: /usr/lib/objrepos mpnp.obj	NONE
Path: /etc/objrepos mpnp.obj	NONE
Path: /usr/share/lib/objrepos mpnp.data	*prereq mpnp.obj v=01 r=01

Figure 12-19. Sample List of Prerequisites for Software Components

List Dependents of a Software Component

To list the dependents of selected software components:

1. Select **List Dependents of a Software Component**.
2. Press **F9 (Esc + 9)** to select each software component on the selector screen that follows. Press **Enter** to record the selections.
3. Press **Enter** to execute the function.

The selected software components are listed with their dependents. Figure 12-20 is an example showing the dependents for the mpnp component.

Name	Dependents
<Name> is a prerequisite of <Dependents>	
Path: /usr/lib/objrepos mpnp.obj	mpnp.obj 01.01.0000.0001.NP61001 mpnp.obj 01.01.0000.0002.NP61002 mpnp.obj 01.01.0000.0003.NP61003
Path: /etc/objrepos mpnp.obj	mpnp.obj 01.01.0000.0001.NP61001 mpnp.obj 01.01.0000.0002.NP61002 mpnp.obj 01.01.0000.0003.NP61003
Path: /usr/share/lib/objrepos mpnp.data	NONE

Figure 12-20. Sample List of Dependents for Software Components

View ID of a Software Component

To list the software IDs for selected software components:

1. Select **View ID of a Software Component**.
2. Press **F9 (Esc + 9)** to select each software component on the selector screen that follows. Press **Enter** to record the selections.
3. Press **Enter** to execute the function.

The selected software components are listed with their product IDs, feature IDs, and vendor code, if applicable. Figure 12-21 is an example showing software IDs for the mpnp component.

Name	Vendor Code	Product Id	Feature Id	Product Name
Path: /usr/lib/objrepos mpnp.obj		5648-01600	0000	mpnp
Path: /etc/objrepos mpnp.obj		5648-01600	0000	mpnp
Path: /usr/share/lib/objrepos mpnp.data		5648-01600	0000	mpnp

Figure 12-21. Sample List of Files for Software Components

View History of a Software Component

To list the history information for selected software components:

1. Select **View History of a Software Component**.
2. Press **F9 (Esc + 9)** to select each software component on the selector screen that follows. Press **Enter** to record the selections.
3. Press **Enter** to execute the function.

The selected software components are listed with their fix IDs, release level, fix status, last action taken, date and time of last action, and the userid of the person who performed the last action. Figure 12-22 on page 12-39 is an example showing history information for the mpnp component.

Name	Fix Id	Release	Status	Action	Date	Time	User Name
Path: /usr/lib/objrepos mpnp.obj		01.01.0000.0000	COMPLETE	COMMIT	09/26/92	16:29:09	root
Path: /etc/objrepos mpnp.obj		01.01.0000.0000	COMPLETE	COMMIT	09/26/92	16:38:33	root
Path: /usr/share/lib/objrepos mpnp.data		01.01.0000.0000	COMPLETE	COMMIT	09/26/92	16:45:37	root

Figure 12-22. Sample List of History Information for Software Components

Verify a Software Component

When software changes are installed, the new files are verified. When the Software Installation and Maintenance Facility verifies a software component, it checks to see whether the component has been changed or corrupted. The software files are checked for the correct length and for the accuracy of the VPD. The facility compares the calculated values to the expected values for differences. If any errors are reported during the verification step, it may be necessary to reinstall the software component or update it. The software files were probably corrupted during the transfer to the IBM 6611.

There may be a situation in which it is necessary to verify a software component at some time after the installation. The component may not verify. However, you may want to make the changed component, the new verify standard.

To verify a software component:

1. Select **Verify a Software Component**
2. Press **F9 (Esc + 9)** to select each software component to verify on the selector screen that follows. Press **Enter** to record the selections.
3. A dialog screen follows with the option, Make changed software the new verify standard. Press **Tab** to toggle between yes and no in the entry field.

Figure 12-23 displays some example output from the software verification test. Output is displayed only for files that fail the test.

```
Size of /etc/promon is 20005, expected value was 18897.
Size of /usr/bin/mnptar is 38911, expected value was 37839.
Size of /usr/bin/mnptrace is 40589, expected value was 40077.
The checksum for file /usr/lib/mnptrace is 9550, expected value is 55691
Size of /usr/lpp/diagnostics/bin/diagrpt is 4725, expected value was 3162.
Size of /usr/lpp/diagnostics/bin/diags is 12672, expected value was 10336.
Size of /usr/lpp/diagnostics/bin/ucfgvpd is 15989, expected value was 20404.
```

Figure 12-23. Software Verification Output Example

Exporting the Software Vital Product Data

To export the software vital product data using the System Manager:

1. Select **Software Installation and Maintenance** from the main menu.
2. Select **View Software Vital Product Data** on the next menu.
3. Select **Export Software Vital Product Data** on the next menu.
4. Select an Export method from the selector screen.
 - FTP
 - Modem
 - DOS diskette
 - UNIX diskette.
5. With each of these file transfer methods, a selector screen appears requesting the name of the file to be transferred. Select the name of the software VPD file.
 - Transferring files with FTP requires you to give the host name and a userid at the destination node on the dialog screen. You are prompted for the password for the userid.
 - Transferring files to a DOS diskette requires you to give the name of the file on the DOS diskette.
 - Transferring files to a UNIX diskette requires you to specify whether to *append* the file to the end of the diskette or to place it as the only file on the diskette, *create*.

Figure 12-24 shows an example of exporting the list of all installed software to a DOS diskette.

Free space: 1334272 bytes
The file softall.list has been exported to soft.all on the DOS diskette.

Figure 12-24. Example of Export Software Vital Product Data to DOS Diskette

Chapter 13. Using Concurrent Diagnostics and Hardware Vital Product Data

Running Concurrent Hardware Diagnostics	13-2
From a Direct-Attached ASCII Terminal	13-2
From a Modem-Attached ASCII Terminal	13-5
From a Workstation on the IP Network	13-5
Hardware VPD Format	13-6
Viewing Hardware Component Information	13-7
Listing Supported Devices	13-9
Listing Defined Devices	13-10
List All Installed Devices	13-11
View Characteristics of a Defined Device	13-11
Viewing Hardware Vital Product Data	13-12
Updating the Hardware VPD after Configuration Changes	13-12
Exporting the Hardware Vital Product Data	13-13

Running Concurrent Hardware Diagnostics

Concurrent hardware diagnostics are diagnostics that can be run while the system is operating. They are designed to test as much of the system, or specified resource, as possible without interfering with system operations. To accomplish this, it is necessary to limit diagnostic testing. If the resource cannot be totally tested in this mode because the resource is in use by the system, a message is displayed informing you of this.

You have the option of stopping some of the system in order to free the resource for more complete testing. You can use the facilities of the System Manager to perform an orderly shutdown of the system and test it in stand-alone mode.

Running concurrent diagnostics requires either an ASCII terminal or terminal emulator attached directly or via a modem to the S1 or S2 EIA 232 serial ports, or a remote workstation attached through the IP network.

Only a controlling user can run hardware diagnostics. See "Logging In to an IBM 6611" on page 9-23 for information about controlling userids.

From a Direct-Attached ASCII Terminal

When an ASCII terminal or terminal emulator is attached directly to the S1 or S2 serial port of an operational IBM 6611, a login screen appears. Log in to the IBM 6611 using a controlling userid and password. Select the correct terminal type when prompted. The System Manager main menu appears.

1. Select **Concurrent Hardware Diagnostics** from the main menu.
2. The Diagnostic Operating Instructions screen is displayed. Press **Enter** to continue. Figure 13-1 shows the first screen of the Diagnostics Programs.

```
LICENSED MATERIALS - PROPERTY OF IBM.  
IBM 6611 Network Processor DIAGNOSTICS VERSION 1.0  
(C) COPYRIGHTS BY IBM AND BY OTHERS 1982, 1992.  
ALL RIGHTS RESERVED.  
US GOVERNMENT USERS RESTRICTED RIGHTS -  
USE, DUPLICATION OR DISCLOSURE RESTRICTED  
BY GSA ADP SCHEDULE CONTRACT WITH IBM CORP.
```

DIAGNOSTIC OPERATING INSTRUCTIONS

These program contain diagnostics and service aids for the system. These procedures should be used whenever problems with the system occur which have not been corrected by any software application procedures available. In general, the procedures will run automatically. However, sometimes you will be required to select options, inform the system when to continue, do simple tasks, and exchange diskettes.

Several keys are used to control the procedures:

- The Enter key continues the procedure or performs an action
- The Backspace key allows keying errors to be corrected.
- The cursor keys are used to select an option.

Press the F3 key to exit or press Enter to continue.

Figure 13-1. First Screen of Diagnostics Programs

3. On the FUNCTION SELECTION screen, select **Diagnostic Routines**. Figure 13-2 shows the FUNCTION SELECTION screen for concurrent hardware diagnostics.

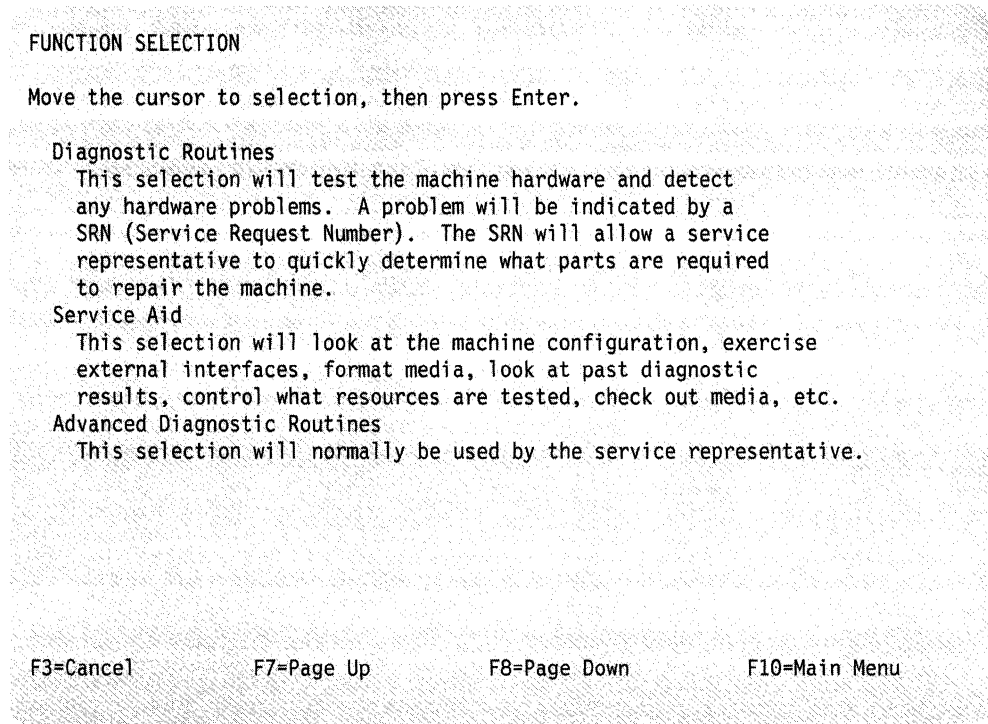


Figure 13-2. FUNCTION SELECTION Screen

4. You receive the DIAGNOSTIC MODE SELECTION screen. Figure 13-3 on page 13-4 shows an example of the DIAGNOSTIC MODE selection screen. Select either **System Verification** or **Problem Determination**.

System Verification checks the correct operation of the system after repairs have been completed. Problem Determination tests the system when a problem is suspected. Problem Determination, in addition to running the hardware diagnostics, analyzes the error log to determine if there have been system errors over the past 24 hours. Whichever mode is selected, the next menu provides a list of the components that can be tested.

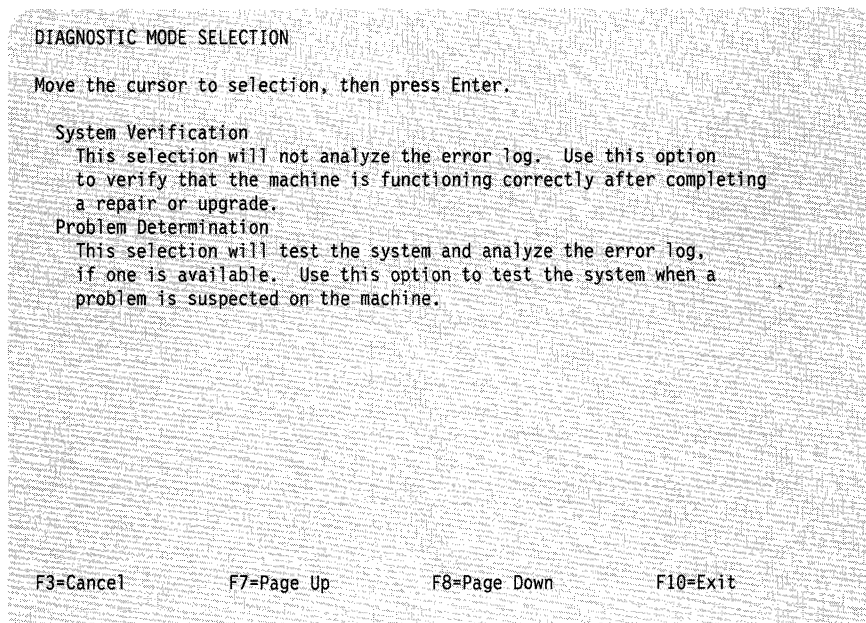


Figure 13-3. Diagnostic Mode Selection Screen

Figure 13-4 displays an example of the DIAGNOSTIC SELECTION screen.

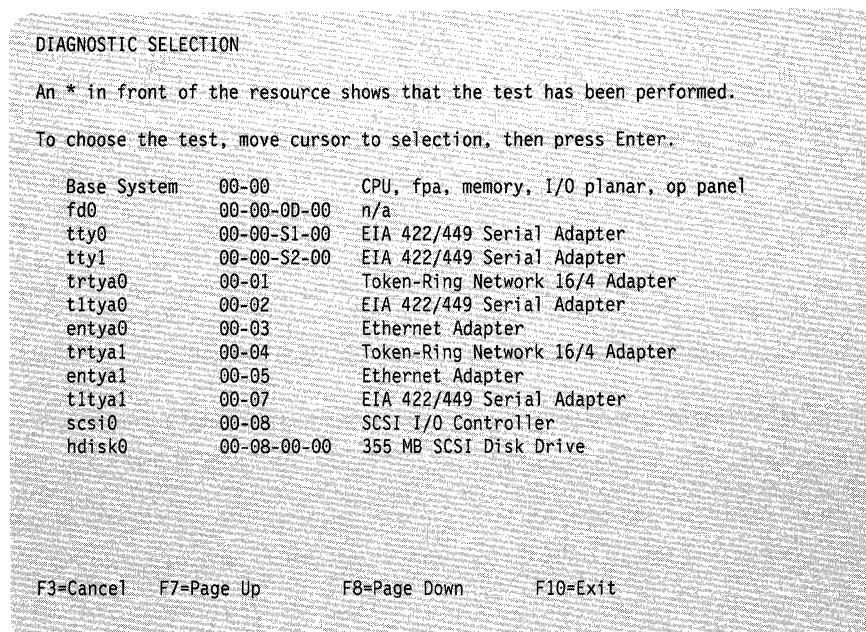


Figure 13-4. Example of Diagnostic Selection Screen in the Diagnostics Program

5. Select the component to be tested by moving the cursor up or down using the up-arrow or the down-arrow keys, and press **Enter** when the cursor is at the correct position.

To exit from any menu to the previous menu, press **F3 (Esc + 3)**.

From a Modem-Attached ASCII Terminal

In order for diagnostics testing to be run from a modem-attached terminal, there must be at least one IBM 6611 on the IP network with a modem attached to either its S1 or S2 serial port. This does not have to be the same IBM 6611 needing to be tested. The modem-attached terminal must be an ASCII terminal or terminal emulator with a communication package capable of dialing out to the IBM 6611 with the modem. The telephone number, baud rate, a configured userid, and password must be known for the IBM 6611 with the modem. The host name or IP address and a controlling userid and password must be known for the IBM 6611 to be tested.

To test an IBM 6611 without a modem:

1. With the terminal or terminal emulator and its modem set to the same baud rate and settings as the modem attached to the IBM 6611, use the instructions for the modem and terminal to dial into the IBM 6611 as you would a remote host. See "Using a Modem" on page 9-17 for information about using a modem.
2. Log in to the IBM 6611 using a controlling userid and password. Specify the correct terminal type.
3. Select **Remote Accesses to Other Nodes** from the System Manager main menu. Select **Issue Remote Login to Any IP Node** from the next menu. You receive a dialog screen. Specify the host name or IP address of the IBM 6611 needing to be tested. Specify a userid configured at that IBM 6611. Press **Enter** and you are prompted for the password. After entering the password, you are logged in to the IBM 6611 needing to be tested.
4. From the main menu of the System Manager, select **Concurrent Hardware Diagnostics**. The rest of the procedure is the same as for a direct-attached ASCII terminal. See "From a Direct-Attached ASCII Terminal" on page 13-2 for more information about accessing concurrent mode diagnostics.

To test an IBM 6611 with a modem:

1. With the terminal or terminal emulator and its modem set to the same baud rate and settings as the modem attached to the IBM 6611, use the instructions for the modem and terminal to dial into the IBM 6611 as you would a remote host. See "Using a Modem" on page 9-17 for information about using a modem.
2. Log in to the IBM 6611 using a controlling userid and password. Specify the correct terminal type.
3. From the main menu of the System Manager, select **Concurrent Hardware Diagnostics**. The rest of the procedure is the same as for a direct-attached ASCII terminal. See "From a Direct-Attached ASCII Terminal" on page 13-2 for more information about accessing concurrent mode diagnostics.

From a Workstation on the IP Network

From any workstation on the IP network, you can remotely run concurrent diagnostics on an IBM 6611 using a TELNET session. The hostname or IP address and a controlling userid and password must be known for the IBM 6611 to be tested. Type **telnet <hostname or IP address>** to begin the TELNET session. Log in using the controlling userid and password when prompted. Specify the terminal type, if prompted. See "Using TELNET" on page 9-8 for more details about TELNET sessions. Control is passed to the System Manager, which displays a login screen. Then, operation is the same as for a direct-attached ASCII terminal. See "From a Direct-Attached ASCII Terminal" on page 13-2 for more information about accessing concurrent mode diagnostics.

Hardware VPD Format

There is a facility that manages the hardware components of the IBM 6611. There are records maintained in the vital product data (VPD) repository for each supported, defined, and installed hardware component. The record layout is as follows:

Hardware Component	A 2-byte field that uniquely identifies the hardware component.
Component Description	A brief description of the part: for example, Ethernet Adapter.
FRU Number	The FRU number is an 8-character ASCII entry that defines the part number used by field service to order a replacement part. It is usually different from the manufacturing part number.
Part number	An 8-character ASCII field that contains the manufacturing part number that identifies the hardware element. This is the number used by manufacturing and development.
Engineering Change (EC) Level	An 8-character ASCII field used by manufacturing and development that specifically identifies the maintenance level of the hardware element.
Manufacturer	The manufacturer descriptor field is a 6-byte ASCII field. Components manufactured by IBM use "IBM" for the first three characters. The next 3 characters are alphanumeric and are a code assigned to each IBM location, for example: RTP is assigned code 023. Vendor manufacturers are identified by a 6-digit number assigned by the purchasing department when a contract is established. An abbreviation for the IBM location establishing the contract is concatenated to the purchase order number.
Serial Number	The serial number is specified as an 8-character ASCII field in the range from 00000000 to ZZZZZZZZ. This number is required to allow you to track assets and allows IBM to track components in the field for machine control purposes.
ROM Level and ID	The data portion of this descriptor is ASCII and is a minimum of 4 characters. Optionally, a second field of variable length information specifies the ROM ID. This additional information is required if the adapter contains more than one ROM module.
Loadable Microcode Level	The level of microcode that exists in the adapter.
Network Address (Token Ring and Ethernet)	The 6-byte universal address for the network interfaces on the hardware element that support universally assigned network addresses. This includes all the LAN adapters in the IBM 6611. There is one entry for each network interface on the adapter.

Slot Location Data is in ASCII. A number from 0 to 7 that indicates the physical slot in which a piece of hardware resides.

Available for Adapter-Specific Use (Z0 L – ZZ L)

Displays various adapter specific information such as the adapter ID. The amount of information varies according to the adapter.

When you display the hardware VPD for most items, you receive:

- Hardware component
- Slot location
- Component description.

Hardware Component	Slot Location	Component Description
fpa0	00-00	Floating Point Processor
bus0	00-00	Micro Channel Bus
fd0	00-00-oD-oo	Diskette Drive

Some hardware components will also display a list of other VPD items, where the information is available. For example:

Hardware Component	Slot Location	Component Description
trtya0	00-01	Token-Ring Network 16/4 Adapter
trty0	00-01-00	Token-Ring Network 16/4 Adapter port

```
Device Specific.(Z0).....{
Network Address.....08005A13006A
Part Number.....93F1146
EC Level.....C40140
FRU Number.....93F3066
Serial Number.....000106
Displayable Message.....6611 Token-Ring Network 16/4 Adapter
Manufacturer.....RAL7868898
Device Driver Level.....00
Diagnostic Level.....00
```

Viewing Hardware Component Information

Using the System Manager or the command primitives, you can view information about the hardware components of the IBM 6611. You can list all the supported, defined, and installed hardware components. Characteristics about defined devices can be listed. VPD is available for all installed devices.

Supported devices are the devices allowed on the IBM 6611 but not necessarily present, configured, or enabled.

Defined devices are supported devices that exist at different status levels. The status levels are:

Available The device is present, configured, and enabled.

Defined The device is configured, but it is not enabled. Defined does not necessarily mean that the device is present. The device may have been moved or removed, and the VPD remains from a previous configuration. Select the **Update Hardware Vital Product Data After Configuration Changes** menu item to match the VPD with the actual hardware setup.

Stopped The device is not operating. Either it is not configured or contains an error. Contact an IBM service personnel or select **Update Hardware Vital Product Data After Configuration Changes** to remove this device.

Installed devices are devices that are present and defined. Figure 13-5 displays the Hardware Vital Product Data menu.

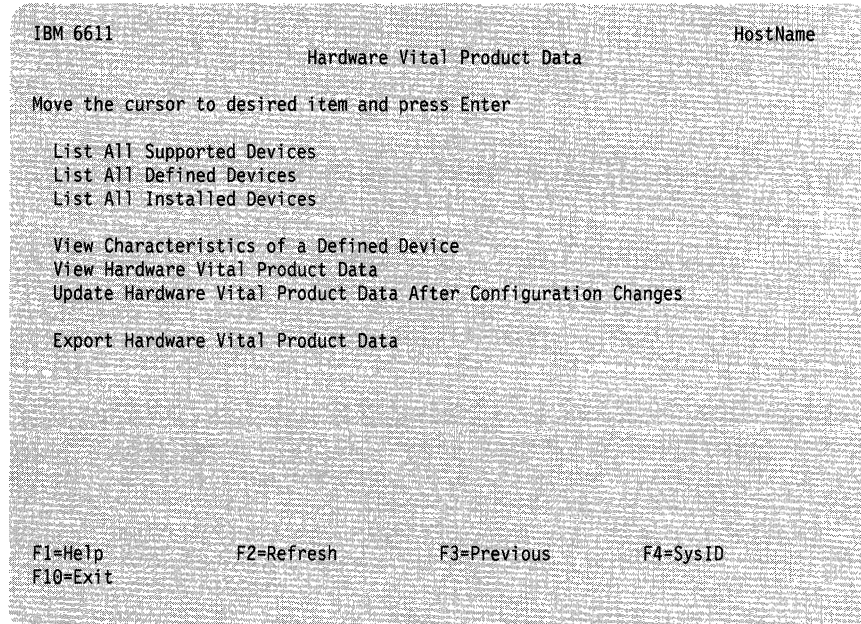


Figure 13-5. Hardware Vital Product Data Menu

To obtain the hardware component information from the System Manager:

1. Select **Hardware Vital Product Data** from the main menu.
2. Select one of the top five menu items:

List All Supported Devices
List All Defined Devices
List All Installed Devices
View Characteristics of a Defined Device
View Hardware Vital Product Data

With each menu item, you can send the output to the screen or to the transfer directory.

See these pages for more information about the individual menu items:

Listing Supported Devices	13-9
Listing Defined Devices	13-10
List All Installed Devices	13-11
View Characteristics of a Defined Device	13-11
Viewing Hardware Vital Product Data	13-12

These tasks can also be invoked using command primitives. See “Hardware Command Primitives” on page 8-57 for information about the command primitives.

Listing Supported Devices

The List All Supported Devices menu item generates a list of all the supported hardware devices along with their class, type, subclass, and description.

Figure 13-6 shows an example of the output.

Class	Type	Subclass	Description
adapter	enty	mca	Ethernet Adapter
adapter	eu	mca	Async Expansion Adapter
adapter	fda	sio	Standard I/O Diskette Adapter
adapter	fda_2	sio	Standard I/O Diskette Adapter
adapter	hscsi	mca	SCSI I/O Controller
adapter	hscsi	sio	Standard SCSI I/O Controller
adapter	mpqp	mca	6611 4-Port SDLC Adapter
adapter	pscsi	sio	Standard SCSI I/O Controller
adapter	sla	sio	Standard I/O Serial Port 1
adapter	sla_1	sio	Standard I/O Serial Port 1
adapter	s2a	sio	Standard I/O Serial Port 2
adapter	s2a_1	sio	Standard I/O Serial Port 2
adapter	sio	mca	Standard I/O Planar
adapter	sio_1	mca	Standard I/O Planar
adapter	sio_2	mca	Standard I/O Planar
adapter	tlty	mca	EIA 422/449 Serial Adapter
adapter	tlty	mca	V.35/V.36 Serial Adapter
adapter	trty	mca	Token-Ring Network 16/4 Adapter
adapter	x25	mca	X.25 Adapter
bus	mca	sys	Micro Channel Bus
disk	badisk	mca	Direct Attached Disk Drive
diskette	fd	siofd	Diskette Drive
dlc	ethernet	dlc	Standard Ethernet Data Link Control
dlc	IEEE_ethernet	dlc	IEEE Ethernet(802.3) Data Link Control
dlc	sdlc	dlc	SDLC Data Link Control
dlc	tokenring	dlc	Token-Ring Data Link Control
dlc	x25_qllc	dlc	X.25 QLLC Data Link Control
entypport	port	enty	Ethernet Adapter Port
fpa	fpa1	sys	Floating Point Processor
if	te	TE	6611 Ethernet Network Interface
if	tk	TK	6611 16-4 Token-Ring Network Interface
if	to	TO	6611 2-Port Serial Network Interface
if	xt	XT	6611 X.25 Network Interface
ioplanar	ioplanar	sys	I/O Planar
ioplanar	ioplanar_1	sys	I/O Planar
ioplanar	ioplanar_2	sys	I/O Planar
logical_volume	lvtype	lvsubclass	Logical Volume
logical_volume	vgtype	vgsubclass	Volume Group
lvm	lvdd	lvm	Logical Volume Interface
memory	memory	sys	Memory Card
memory	sim	sys	Memory SIMM
mpqpport	port	mpqp	IBM 6611 4-Port SDLC Adapter Port
planar	sysplanar1	sys	CPU Planar
pty	pty	pty	Asynchronous Pseudo-Terminal
swap	paging	nfs	NFS Swap Device
sys	aio	node	Asynchronous I/O
sys	sys	node	System Object
sysunit	sysunit	sys	6611 Network Processor
tltyport	port	tlty	EIA 422/449 Serial Adapter Port
tltyport	port	tlty	V.35/V.36 Serial Adapter Port
tcPIP	inet	TCPIP	Internet Network Extension
tm SCSI	hscsi	scsi	SCSI I/O Controller Initiator Device
trtyport	port	trty	Token-Ring Network 16/4 Adapter Port
tty	tty	rs232	Asynchronous Terminal - EIA232
tty	tty	rs422	Asynchronous Terminal - EIA422

Figure 13-6. Listing Supported Devices Output

Listing Defined Devices

The List All Defined Devices menu item generates a list of all the defined hardware devices along with their status, location, and description. Figure 13-7 shows an example of the output.

name	status	location	description
sys0	Available	00-00	System Object
sysplanar0	Available	00-00	CPU Planar
ioplanar0	Available	00-00	I/O Planar
bus0	Available	00-00	Micro Channel Bus
sio0	Available	00-00	Standard I/O Planar
sysunit0	Available	00-00	IBM 6611 Network Processor
fpa0	Available	00-00	Floating Point Processor
mem0	Available	00-00	16-MB Memory Card
fda0	Available	00-00-00	Standard I/O Diskette Adapter
sa0	Available	00-00-S1	Standard I/O Serial Port 1
sa1	Available	00-00-S2	Standard I/O Serial Port 2
fd0	Available	00-00-00-00	Diskette Drive
hdisk0	Available	00-08-00-00	355 MB SCSI Disk Drive
lvdd	Available		N/A
tty0	Available	00-00-S1-00	Asynchronous Terminal
rootvg	Defined		Volume Group
hd6	Defined		Logical Volume
hd61	Defined		Logical Volume
hd5	Defined		Logical Volume
hd7	Defined		Logical Volume
hd8	Defined		Logical Volume
hd4	Defined		Logical Volume
hd2	Defined		Logical Volume
hd9var	Defined		Logical Volume
hd3	Defined		Logical Volume
hd1	Defined		Logical Volume
slc0	Available	00-00	Serial Optical Link Chip
ppa0	Available	00-00-0P	Standard I/O Parallel Port Adapter
pty0	Available		Asynchronous Pseudo-Terminal
inet0	Available		Internet Network Extension
aio0	Defined		Asynchronous I/O
tty1	Available	00-00-S2-00	Asynchronous Terminal
trtya0	Available	00-01	Token-Ring Network 16/4 Adapter
entya0	Available	00-03	Ethernet Adapter
entya1	Available	00-04	Ethernet Adapter
entya2	Available	00-05	Ethernet Adapter
tltya0	Available	00-06	EIA 422/449 Serial Adapter
tlty0	Available	00-06-01	6611 Serial Adapter Port
tlty1	Available	00-06-02	6611 Serial Adapter Port
trty0	Available	00-01-01	Token-Ring Network 16/4 Adapter Port
enty0	Available	00-03-01	Ethernet Adapter Port
enty1	Available	00-04-01	Ethernet Adapter Port
enty2	Available	00-05-01	Ethernet Adapter Port

Figure 13-7. Example List of Defined Devices

List All Installed Devices

The List All Installed Devices menu item generates a list of all installed hardware devices along with their location and description. Figure 13-8 shows an example of the output.

The following resources are installed on the machine.

+/- = Added or deleted from Diagnostic Test List.

* = NOT supported by Diagnostics.

+ sysplanar0	00-00	CPU Planar
+ fpa0	00-00	Floating Point Processor
* slc0	00-00	Serial Optical Link Chip
+ mem0	00-00	16 MB Memory Card
+ ioplanar0	00-00	I/O Planar
* bus0	00-00	Micro Channel Bus
* sio0	00-00	Standard I/O Planar
+ fda0	00-00-0D	Standard I/O Diskette Adapter
+ fd0	00-00-0D-00	Diskette Drive
* ppa0	00-00-0P	Standard I/O Parallel Port Adapter
+ sa0	00-00-S1	Standard I/O Serial Port 1
+ tty0	00-00-S1-00	Asynchronous Terminal
+ sa1	00-00-S2	Standard I/O Serial Port 2
+ tty1	00-00-S2-00	Asynchronous Terminal
+ trtya0	00-01	Token-Ring Network 16/4 Adapter
+ entya0	00-03	Ethernet Adapter
+ entya1	00-04	Ethernet Adapter
+ entya2	00-05	Ethernet Adapter
+ tltya0	00-06	EIA 422/449 Serial Adapter
+ scsi0	00-08	SCSI I/O Controller
+ hdisk0	00-08-00-00	355 MB SCSI Disk Drive
* sysunit0	00-00	IBM 6611 Network Processor
* tlty0	00-06-01	EIA 422/449 Serial Adapter Port
* tlty1	00-06-02	EIA 422/449 Serial Adapter Port
* trty0	00-01-01	Token-Ring Network 16/4 Adapter Port
* enty0	00-03-01	Ethernet Adapter Port
* enty1	00-04-01	Ethernet Adapter Port
* enty2	00-05-01	Ethernet Adapter Port

Figure 13-8. List of Installed Devices Example

View Characteristics of a Defined Device

The View Characteristics of a Defined Device menu item generates information about a configured and defined hardware device. You can select the hardware device from a selector screen. The device name is listed along with its description, status, location, and details. Figure 13-9 displays an example of the output obtained for the Ethernet Adapter.

name	description	status	location
enty1	Ethernet Adapter Port	Available	00-04-00

description	value
RECEIVE DATA TRANSFER OFFSET	32
Enable ALTERNATE ETHERNET address	no
ALTERNATE ETHERNET address	0x

Figure 13-9. View Characteristics of a Defined Device Example

Viewing Hardware Vital Product Data

The VPD of all installed hardware devices is listed. For some devices, there is very little or no VPD given. For other devices, complete VPD is provided. Figure 13-10 shows an example of the output for the Token-Ring Network 16/4 Adapter and Ethernet Adapter.

INSTALLED RESOURCE LIST WITH VPD

The following resources are installed on your machine.

```
trtya0          00-01          Token-Ring Network 16/4 Adapter
trty0           00-01-00       Token-Ring Network 16/4 Adapter port
    Device Specific.(Z0).....{
    Network Address.....08005A13006A
    Part Number.....93F1146
    EC Level.....C40140
    FRU Number.....93F3066
    Serial Number.....000106
    Displayable Message.....6611 Token-Ring Network 16/4 Adapter
    Manufacturer.....RAL7868898
    Device Driver Level.....00
    Diagnostic Level.....00
    ROS Level and ID.....00
    Loadable Microcode Level....00

entya0          00-03          Ethernet Adapter
enty0           00-03-00       Ethernet Adapter port
    Device Specific.(Z0).....z
    Network Address.....08005A13224D
    Part Number.....93F1145
    EC Level.....C40140
    FRU Number.....93F3067
    Serial Number.....000589
    Displayable Message.....Ethernet Adapter
    Manufacturer.....RAL7868898
    Device Driver Level.....00
    Diagnostic Level.....00
    ROS Level and ID.....00
    Loadable Microcode Level....00
```

Figure 13-10. Viewing Hardware VPD Example

Updating the Hardware VPD after Configuration Changes

When hardware devices are added or removed from the IBM 6611, the hardware component information needs to be updated to reflect the change. The IBM 6611 can check for changes in its hardware configuration using the System Manager or the command primitives.

Using the System Manager:

1. Log in using a controlling userid.
2. Select **Hardware Vital Product Data** from the main menu.
3. Select **Update Hardware Vital Product Data After Configuration Changes** from the next menu.

If the IBM 6611 finds differences between the existing hardware VPD and the present hardware configuration, a menu is displayed. The menu identifies the items that have different VPD and configuration information. A list of possible scenarios causing the mismatch is provided. Select the one that explains the mismatch.

When no changes are found by the Update Hardware Vital Product Data After Configuration Changes, the system returns to the Hardware Vital Product Data menu screen. Figure 13-11 displays an example of this report. In the example, an Ethernet Adapter was removed.

```

MISSING RESOURCE                                     801020

The following resource was detected previously, but is not detected now:

- entya 0          00-04          Ethernet Adapter

Has the resource been removed from the screen, moved to another location
or address, or turned off?

The resource has NOT been removed from the system, moved to
another location or address, or turned off.
This selection will determine why the resource was not detected.
The resource has been removed from the system and should be
removed from the system configuration.
The resource has been moved to another location and should be
removed from the system configuration.
The resource has been turned off and should be removed from
the system configuration.
The resource has been turned off but should remain in the
system configuration.

F3=Cancel      Esc+7=Page Up      Esc+8=Page Down      Esc+0=Exit

```

Figure 13-11. Update Hardware VPD after Configuration Changes Example Output

Exporting the Hardware Vital Product Data

To export the hardware VPD using the System Manager:

1. Select **Hardware Vital Product Data** from the main menu.
2. Select **Export Hardware Vital Product Data** on the next menu.
3. Select an Export method from the selector screen.
 - FTP
 - Modem
 - DOS diskette
 - UNIX diskette.
4. With each of these file transfer methods, a selector screen appears requesting the name of the file to be transferred. Select the name of the hardware VPD file.
 - Transferring files with FTP requires you to give the host name and a userid at the destination node on the dialog screen. You are prompted for the password for the userid.
 - Transferring files to a DOS diskette requires you to give the name of the file on the DOS diskette.
 - Transferring files to a UNIX diskette requires you to specify whether to *append* the file to the end of the diskette or to place it as the only file on the diskette, *create*.

Figure 13-12 shows an example of exporting hardware vital product data using FTP.

```
Enter password for netman
(user enters password invisibly here)
Connected to nv6host.
220 nv6host FTP server (Version 4.1 Sat Nov 23 12:52:09 CST 1991) ready.
331 Password required for netman.
230 User netman logged in.
Local directory is now /tmp/hold/transfer
200 PORT command successful.
150 Opening data connection for vpd_supdev.list
226 Transfer complete.
748 bytes sent in 0.07346 seconds (9.944 Kbytes/s)
221 Goodbye.
```

Figure 13-12. Example of Export Hardware Vital Product Data Output Using FTP

Chapter 14. Using the System Manager to Configure the IBM 6611

About This Chapter	14-4
Updating Configuration Parameters	14-4
Configuration Objects	14-7
Configuration Procedure	14-8
Initial Configuration Using a Diskette	14-11
Initial Configuration without Using a Diskette	14-11
Direct IP Attachment	14-12
Modem Transfer Method	14-12
FTP Transfer Method	14-14
Minimal Configuration Using the System Manager	14-15
Importing and Exporting the Configuration File	14-17
Reinstating a Saved Configuration File	14-19
Working with the Configuration Information Text Files	14-20
Configuration Report	14-20
Configuration Error Message Report	14-22
Configuration Script	14-23
Export Configuration Information	14-25
Box-Level Single Objects	14-26
Parameters for AppleTalk	14-26
APPN Parameters	14-26
APPN Thresholds	14-26
Parameters for BGP	14-26
Protocol Bridging Parameters	14-27
Bridging Spanning Tree Parameters	14-27
Configuration Process Parameters	14-27
DECnet Parameters	14-27
Data Link Switching Parameters	14-28
Parameters for EGP	14-28
Hello Parameters	14-28
IP Parameters	14-28
IPX Parameters	14-29
Software Lock Parameters	14-29
NetBIOS Filter Parameters	14-29
OSPF Parameters	14-29
Protocol – Independent Parameters	14-29
RIP Parameters	14-30
SNA Frame Filter Parameters	14-30
SNMP System Contact	14-30
SNMP System Name	14-30
SNMP System Location	14-30
SNMP Parameters	14-31
Serial Line TTY Parameters	14-31
XNS Parameters	14-31
Transparent Bridging Parameters	14-31
Transparent Bridging Spanning Tree Parameters	14-32
Transparent Bridging Destination Values	14-32
XNS Static Route Tables Parameters	14-32
APPN Parameters for Threshold (Accessed from System Manager-ONLY)	14-33
Constrained Threshold	14-33
Critical Threshold	14-33
Retry Counter	14-33
Port-Level Single Objects	14-34

AppleTalk DLCI Available on a Port	14-34
AppleTalk Port Values	14-34
Source Route Bridging Parameters	14-35
DECnet Parameters	14-36
Ethernet Adapter Parameters	14-36
IP Parameters	14-36
IP Filter Parameters	14-36
IPX Parameters	14-37
SDLC Adapter Parameters	14-37
Transparent Bridging Port Parameters	14-38
NetBIOS Packet Forwarding Parameters	14-39
EIA 422/449 Serial Adapter or V.35/V.36 Serial Adapter Port Parameters	14-39
IBM LAN Bridge Parameters	14-39
Frame Relay Parameters	14-40
Point-to-Point Protocol Parameters	14-40
SNA Parameters	14-40
Token-Ring Adapter Parameters	14-40
X.25 Parameters	14-40
X.25 Subscription Parameters	14-41
X.25 Network Tuning Parameters	14-41
X.25 Subscription PVC Default Parameters	14-42
X.25 Subscription SVC Parameters	14-42
XNS Parameters	14-43
Port-Level List Objects	14-43
List of AppleTalk Packet Filters	14-43
List of Additional AppleTalk Zone Names	14-43
List of MAC Input Filters for SRB	14-43
List of Ring Input Filters for SRB	14-44
List of SAP Input Filters for SRB	14-44
List of SNAP Input Filters for SRB	14-44
List of MAC Output Filters for SRB	14-44
List of Ring Output Filters for SRB	14-44
List of SAP Output Filters for SRB	14-44
List of SNAP Output Filters for SRB	14-44
List of Ring Number—DLCI Pairs for SRB	14-44
List of MAC Input Filters for TB	14-45
List of SAP Input Filters for TB	14-45
List of Sliding Window Input Filters for TB	14-45
List of SNAP Input Filters for TB	14-45
List of Logical Ports Number to DLCI Pairs for TB	14-45
List of MAC Output Filters for TB	14-45
List of SAP Output Filters for TB	14-45
List of Sliding Window Output Filters for TB	14-46
List of SNAP Output Filters for TB	14-46
List of DECnet Node to DLCI Mappings	14-46
List of DECnet Packet Filters	14-46
List of Multicast MAC Addresses	14-46
List of IP Destination Address to DLCI Mappings	14-46
List of IP Parameters for X.25	14-47
List of IPX Destination Address to DLCI Mappings	14-47
List of IPX Filters	14-48
List of SNA Stations for Adapter	14-49
List of DLCIs Attached to Frame Relay	14-49
List of SAP Values	14-49
List of X.25 Subscription PVC Parameters	14-49
List of XNS Destination Address to DLCI Mappings	14-50

List of XNS Filters	14-50
Box Level List Objects	14-50
List of Valid Configuration Hosts	14-50
List of DECnet Packet Filters	14-51
List of Participating DLS Routers	14-51
List of GATED Export Parameters	14-51
List of No-HELLO-In/No-HELLO-Out Settings	14-51
List of Hello Source Routers	14-51
List of Hello Trusted Routers	14-52
List of IP Packet Filters	14-52
List of IP Static Routes	14-52
List of Inbound IPX RIP Filter Parameters	14-52
List of Outbound IPX RIP Filter Parameters	14-52
List of IPX Router Filters	14-53
List of IPX SAP Filters	14-53
List of NetBIOS Default Destinations	14-53
List of NetBIOS Destination Name Filters	14-53
List of NetBIOS Source Name Filters	14-53
List of Static Host to Internet Address Mappings	14-53
List of No-RIP-In/No-RIP-Out Settings	14-54
List of RIP Source Routers	14-54
List of RIP Trusted Routers	14-54
List of Remote Name Servers	14-54
List of Remote Time Servers	14-54
List of SNA Default Destinations	14-54
List of SNA Destination Frame Filters	14-54
List of SNA Source Frame Filters	14-55
List of SNMP Clients for Traps	14-55
List of SNMP Communities	14-55
List of Controlling User Names and Passwords	14-55
List of Viewing User Names and Passwords	14-56
List of XNS RIP Inbound Filters	14-56
List of XNS RIP Outbound Filters	14-56
List of XNS RIP Router Filters	14-56
List of Transparent Bridging Filters	14-56

About This Chapter

This chapter explains how to use the System Manager to configure the IBM 6611.

There are two types of configuration files:

Binary configuration file

This file contains the actual configuration. It is created when a user defines configuration parameters from either the Configuration Program or the System Manager. It is transferred between the Configuration Program and the IBM 6611 using one of the following methods:

- Direct connection over an IP network, when the configuration station is an IBM RISC System/6000 workstation.
- The file transfer protocol (FTP), when the configuration station is connected to the same IP network as the IBM 6611.
- The Xmodem protocol, when the configuration station has a modem and a connection to the IBM 6611 through the public switched network.
- A diskette, when there is no remote method available to transfer the file.

Configuration information text files

There are three types of configuration information files:

- Configuration reports
- Configuration error messages
- Configuration script.

The configuration reports contain information about the current configuration. The configuration error messages are sent to the IBM 6611 Error Log by the configuration process and the protocols and adapters. Whenever the System Manager is used to update configuration, a history of the configuration commands issued to change the configuration is kept in the configuration script.

The System Manager configuration facility has three roles:

1. It can be used to update configuration parameters, when the Configuration Program is not available.
2. It is involved in the transfer of the binary configuration file from the Configuration Program to the IBM 6611.
3. It is used to view and transfer the configuration information text files. Only a controlling user can perform configuration tasks from the System Manager.

You must be a controlling user to use the System Manager for most of these configuration tasks.

Updating Configuration Parameters

You can configure the IBM 6611 using either the Configuration Program or the System Manager. The primary method of configuring the IBM 6611 is with the Configuration Program. The alternate method of configuring the IBM 6611 is using the System Manager. It is used mainly for backup purposes if, for any reason, the Configuration Program is not available.

Warning: This method of configuring the IBM 6611 is **not** designed to be the primary method to configure the IBM 6611. There is minimal error checking and no dependency checking. If a parameter or set of parameters is dependent on another set of parameters, no checks are made to see that both sets are configured at the same time. Only experienced IBM 6611 configuration experts should use this method for configuring the IBM 6611.

Only a controlling user can use the System Manager to update configuration parameters.

The System Manager method of configuring the IBM 6611 includes an apply, test, and either commit or reject scenario. The configuration changes are *applied* and *tested* in an actual test environment, and then either *committed* if the changes are approved, or *rejected* if the changes are not approved. Refer to “Configuration Procedure” on page 14-8 for the details of this scenario.

When you begin modifying the system configuration using the System Manager, a local copy of the configuration data is created in the home directory of your userid, which acts as a work file in which any additional configuration modifications are recorded. These changes are not yet part of the system configuration database.

If you want to try out the changes but want to be able to restore the original configuration, you can select **Apply Changes to Configuration Database** from the Adapter and Protocol Configuration menu. This will cause the current configuration to be saved in the home directory of your userid, before the configuration changes from the work file are made a part of the current configuration. At some time later you can decide to commit these changes. You may make additional modifications to the configuration, and apply these changes in an incremental fashion.

If you are satisfied with the changes and want to commit them to the configuration database, selecting Commit Changes to Configuration Database will give you the choice of committing only the previously applied changes or both the previously applied changes and the unapplied changes made from this userid. The System Manager will then make the configuration changes described in the work file a permanent part of the current configuration.

If you want to remove uncommitted configuration changes, selecting Reject Uncommitted Changes to Configuration Database will give you the choice of undoing all your configuration changes since the last commit operation, (both applied and unapplied changes), or to simply discard any changes made since the last apply or commit operation (only unapplied changes).

When you begin to modify the configuration data from a specific userid and a local copy is made, the System Manager will display the modified version, not the current version. Since the local copy is user-specific, changes that have not been applied or committed will only be seen using that particular userid. When the changes have been committed or applied, the System Manager will return to showing the current configuration. This may be confusing if multiple users are modifying or importing configuration data.

You can view the status of your configuration changes by pressing F4 or Esc + 4, from any System Manager menu screen. An example of this screen is shown in Figure 14-1 on page 14-6. When viewing this screen, press **Enter** to return to the System Manager menu screen.

When the System Manager is used to create the latest applied or committed configuration changes, the configuration name has the following format:

localhost(userid) Date Time

The *userid* is the name of the user who made the latest applied or committed configuration changes at the date and time specified.

The configuration status presented is from the perspective of the user who pressed **F4 (ESC + 4) = SysID** to view this information. The configuration status is either **current**, **applied**, **unapplied**, or **partially applied**.

If the status is **current**, then all configuration changes made from the *userid* that you are logged in to have been committed. However, there may be unapplied or applied configuration changes made by a different user. If another user has some applied, but not committed changes, the configuration name will have the localhost format. The *userid* will contain the name of the user who has applied, but not committed the last configuration changes. The only way to determine if there are unapplied configuration changes is to login with each controlling *userid* and press **F4 (ESC + 4) = SysID** to view its configuration status.

If the status is **applied**, then the *userid* that you are logged in to has some applied but not committed configuration changes.

If the status is **unapplied**, then the *userid* that you are logged in to has some unapplied configuration changes.

If the status is partially applied, then the *userid* that you are logged into has some applied and unapplied configuration changes.

If you want to view only the applied or committed changes, log off and log back in with another *userid*. The configuration output produced from the different *userid* will not reflect the unapplied changes made from the previous *userid*. It will reflect all applied changes made from the previous *userid*.

Warning: Please make all System Manager configuration changes from the same controlling *userid* to minimize the chance of overriding another user's configuration changes.

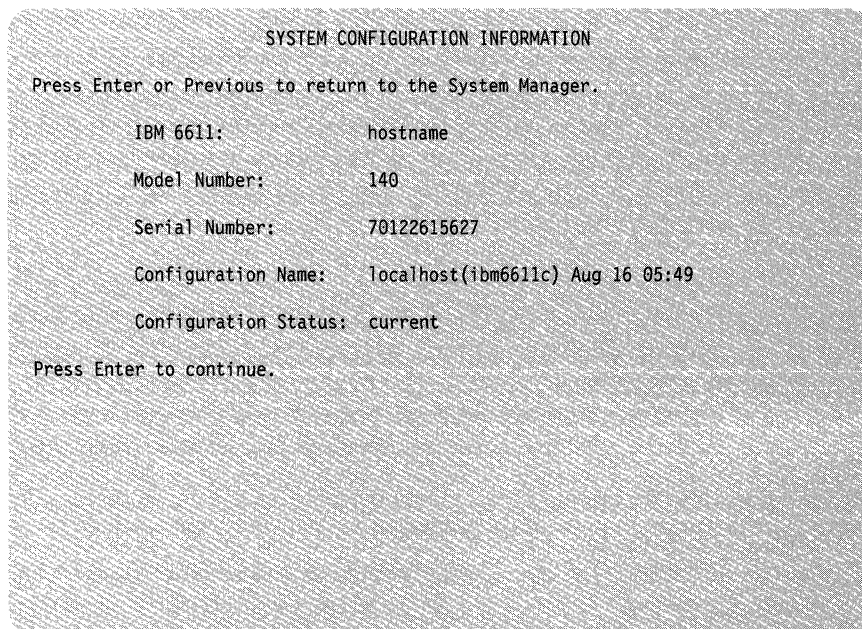


Figure 14-1. System Configuration Information Screen

Configuration Objects

The configuration parameters are separated into logical configuration objects. The configuration parameters associated with any object are related functionally and by data structure type. The System Manager groups these configuration objects both functionally and by data structure type.

If the configuration object is not adapter dependent, it is considered to be a *box-level parameter*. If the configuration object is adapter dependent, it is considered to be a *port-level parameter*. If the configuration object is a single entity, not containing lists, it is called a *single object*. If the configuration object contains multiple occurrences of the same set of parameters, it is called a *list object*.

There are two sets of System Manager configuration commands. The set you choose depends on the type of configuration object data structure. When selecting the correct set of commands, you choose its high-level functional grouping, either box-level or port-level.

Each configuration object in the System Manager is updated as a complete entity on the same dialog screen. The tables at the end of this chapter apply to each configuration object. The tables list the parameters associated with the particular configuration parameter. A page reference is provided for each parameter that has a configuration parameter description in Chapter 3 through Chapter 6. These tables should help you become familiar with the location of configuration objects in the System Manager Configuration Facility.

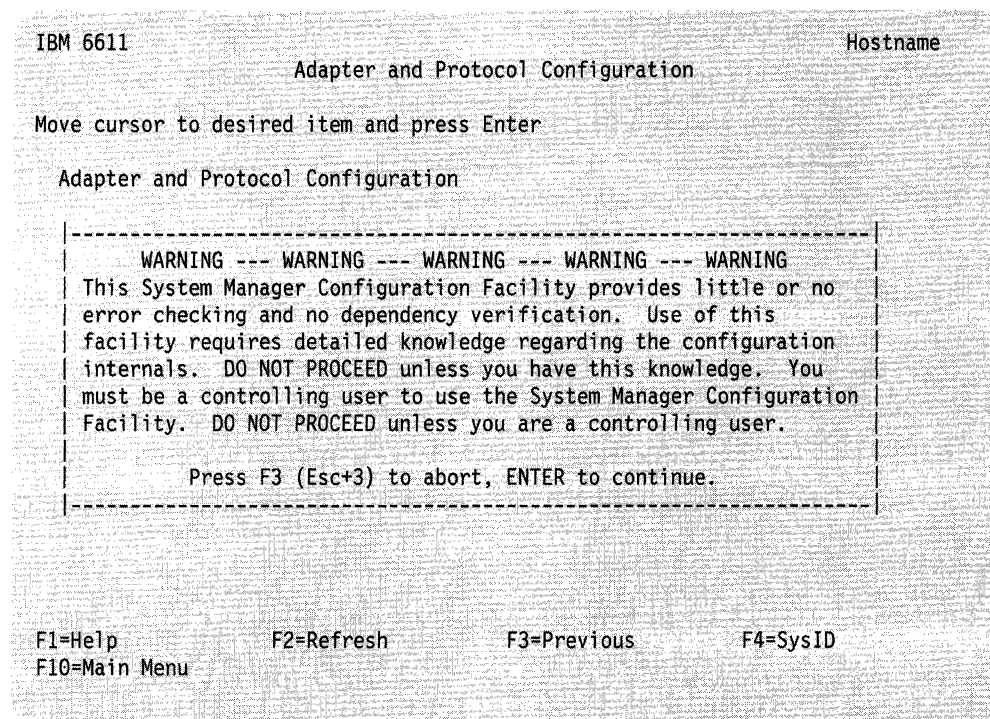


Figure 14-2. Warning Screen for the Adapter and Protocol Configuration Menu Item

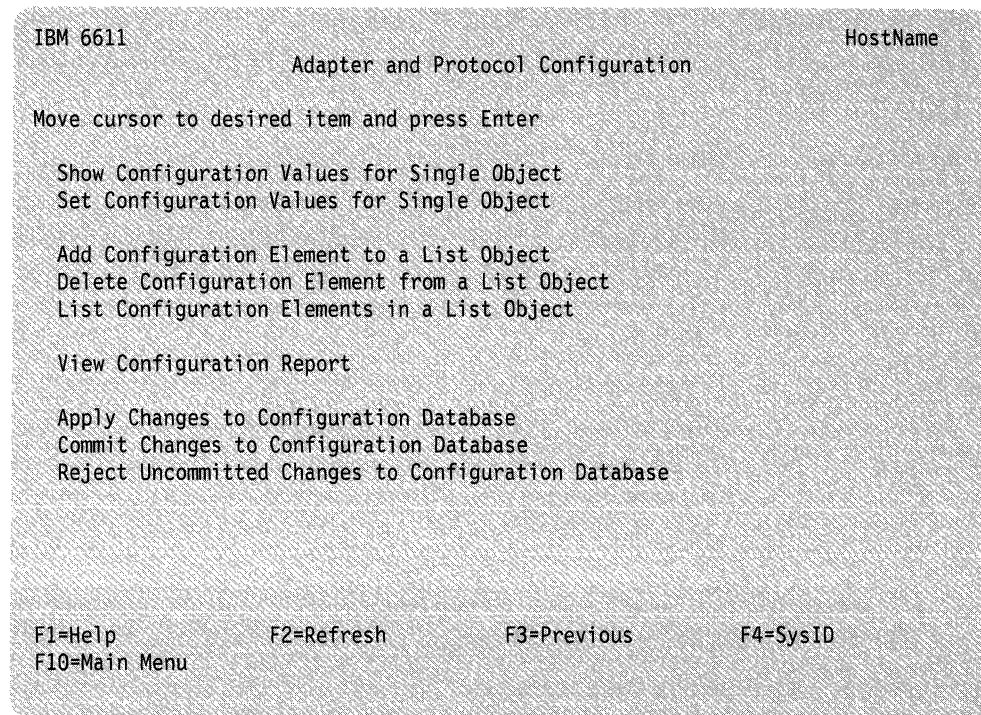


Figure 14-3. Menu Screen for the Adapter and Protocol Configuration Main Menu Item

Configuration Procedure

Only a controlling user can change the configuration from the System Manager. To change the values of the configuration parameters using the System Manager, perform the following steps after logging in as a controlling user:

- Step 1** Select **Adapter and Protocol Configuration** from the System Manager main menu. A warning screen appears encouraging you to exit, if you are not familiar with the configuration parameters or the System Manager method of configuring the IBM 6611. See Figure 14-2 on page 14-7.
- Step 2** Press **Enter** to proceed to the Adapter and Protocol Configuration main menu. See Figure 14-3.
- Step 3** Use the tables at the end of the chapter starting on page 14-26 to help you locate the configuration object that you want to update.
Note: Determine whether the configuration object is a single object or a list object, and whether it is a box-level object or a port-level object. If you select a port-level object, you also need to know the slot number and the port number of the adapter for which the configuration parameter is being changed. If you are updating a single object, continue with Step 4. If you are updating a list object, go to Step 5.
- Step 4** For a single object, select **Set Configuration Values for Single Objects** to change the values of its parameters. A selector screen appears requesting you to select the functional level of the configuration object. See Figure 14-4 on page 14-9. If you are updating a box-level parameter, go to Step 6. If you are updating a port-level parameter, go to Step 7.

Select Parameter Level		
Move cursor to desired item and press Enter.		
Box Level Parameters		
Port Level Parameters		
F1=Help	F2=Refresh	F3=Previous
F7=Page Up	F8=Page Down	F10=Main Menu

Figure 14-4. Select Parameter Level Selector Screen

- Step 5** For a list object, select **Add Configuration Element to a List Object** to add a new element to the list object. Select **Delete Configuration Element from a List Object** to delete an existing element from the list. A selector screen appears requesting you to select the functional level of the configuration object. Figure 14-4 shows the selector screen for choosing the type of parameter. If you are updating a box-level parameter, continue with Step 6. If you are updating a port-level parameter, go to Step 7.
- Step 6** Select **Box Level Parameter**. Go to Step 8.
- Step 7** Select **Port Level Parameter**. Two more selector screens appear requesting the adapter slot number and the adapter port number for the adapter you are configuring. Only the slots containing installed adapters are shown. Only the possible port numbers for the chosen adapter are shown. See Figure 14-5 and Figure 14-6 on page 14-10 for a sample of these selector screens. Select the correct values based on your hardware configuration.

Adapter Slot Number		
Move cursor to desired item and press Enter.		
Slot 1 :: 6611 X.25		
Slot 2 :: 6611 4-Port SDLC		
Slot 3 :: 6611 2-Port Serial		
Slot 4 :: 6611 Ethernet		
Slot 5 :: 6611 Token-Ring		
Slot 6 :: 6611 Ethernet		
Slot 7 :: 6611 Token-Ring		
F1=Help	F2=Refresh	F3=Previous
F7=Page Up	F8=Page Down	F10=Main Menu

Figure 14-5. Sample Adapter Slot Number Selector Screen

Adapter Port Number		
Move cursor to desired item and press Enter.		
Port 1 Port 2 Port 3 Port 4		
F1=Help	F2=Refresh	F3=Previous
F7=Page Up	F8=Page Down	F10=Main Menu

Figure 14-6. Sample Adapter Port Number Selector Screen

- Step 8** Select the configuration object from the Configuration Data Type selector screen.
- Step 9** A dialog screen appears. The parameters presented are dependent upon the selected object. Press **F1 (Esc + 1)** or use the tables starting on page 14-26 for references to locate details about each parameter. Press **Enter** after changing the parameters.
- Step 10** A command status screen appears. If the process is successful, a *Command: OK* message is displayed. Press **F3 (Esc + 3)** until you return to the Adapter and Protocol Configuration menu. If you received any error messages, try to correct the problem, if you can, or call your IBM service personnel for assistance.
- Step 11** At this point you may want to view the configuration changes that you have made. If the configuration object is a single object, that is, the changes were made using the **Set Configuration Values for Single Objects** menu item, select **Show Configuration Values for Single Objects** to view the changes. Follow the same path through the selector screens to the Configuration Data Type to Show selector screen to view the configuration object.
- If the configuration object is a list object, that is, if the changes were made using either the Add Configuration Element to a List Object or Delete Configuration Element from a List Object menu items, select **List Configuration Elements in a List Object** to view the changes. Follow the same path through the selector screens to the Configuration Data Type to List selector screen to view the configuration object.
- Step 12** If you agree with the new configuration changes that you made, and you want to make them the new configuration, select **Apply Changes to Configuration Database** from the Adapter and Protocol Configuration menu. This selection *applies* the configuration changes. The previous settings of the configuration values are saved. The changed configuration values become the new configuration.
- Warning:** If you updated any configuration parameters that cannot be changed dynamically, either the IBM 6611 is restarted or the protocol with the changed configuration is restarted. See "Configuration Considerations" on page 1-10 for the details about which parameters require restarting the IBM 6611 or system components. Wait a few minutes after selecting to *apply* the configuration changes, before executing other IBM 6611 commands, in case the IBM 6611 is restarted.

Step 13 After operating with the changed configuration, you can accept the new values by committing the new configuration or return to the previous configuration by rejecting the new configuration. To *commit* the configuration changes, select **Commit Changes to Configuration Database** from the main Adapter and Protocol Configuration menu. Any new changes to the configuration that have not been applied are also committed. To *reject* the configuration changes, select **Reject Uncommitted Changes to Configuration Database** from the main Adapter and Protocol Configuration menu. On the selector screen, you can choose to reject only the unapplied changes or both the unapplied changes and applied changes. If you choose the applied and unapplied option, the current configuration is restored to the last committed state. If you choose the unapplied only option, the current configuration is not affected. You cannot reject a configuration that has a time delay configured.

Initial Configuration Using a Diskette

The Configuration Program is used to configure the IBM 6611 initially:

1. The configuration file is created with the Configuration Program and placed on a diskette. See Chapter 2 for instructions about using the Configuration Program.
2. The diskette is carried to the IBM 6611 and placed in the diskette drive.
3. With the key mode switch on the front panel set in the **Normal** position, turn the power switch to ON.

The configuration file is read and the new parameters are used as the current configuration.

Note: To prevent subsequent configurations from this diskette or accidental overwriting of the configuration data, remove the diskette from the diskette drive.

Initial Configuration without Using a Diskette

The System Manager can be used to configure the IBM 6611 minimally so that it can be initially configured from the Configuration Program without using a diskette. There are three methods to transfer the configuration file from the Configuration Program to the IBM 6611 without using a diskette.

1. Direct IP Connection

This method is available using a RISC System/6000 workstation only to perform configuration.

2. Modem Attachment

- A modem must be attached to the configuration workstation and to an IBM 6611 on the network.
- The configuration workstation must also have a communication package that supports call-out and the Xmodem Protocol.
- This method could be used with a PS/2 configuration workstation that has a supported communication package.

3. FTP

- The configuration workstation must be attached to the IBM 6611 through the IP network.
- This method could be used with a PS/2 configuration workstation that has TCP/IP installed.

One of these methods must be available, if you want to perform initial configuration on the IBM 6611 from the Configuration Program without using a diskette.

Direct IP Attachment

This is available only when using a RISC System/6000 configuration workstation attached to the same IP network as the IBM 6611 needing initial configuration. Perform the following steps to configure the IBM 6611 initially over the IP network.

1. The IBM 6611 must be minimally configured for IP. See "Minimal Configuration Using the System Manager" on page 14-15 for details about minimal configuration.
2. See "Direct IP Connection" on page 2-14 for the details about sending the configuration file from the Configuration Program over the direct connection.

Modem Transfer Method

If you are using the modem-attachment method to configure the IBM 6611 initially and the modem is attached to the IBM 6611 needing to be configured, minimal configuration is not necessary. Use the following steps to configure the IBM 6611 initially using the modem connection to send the configuration file.

1. Attach a 2400-bps modem to the EIA 232 S2 serial port on the IBM 6611 (labelled S2 on the Model 120 and the Model 170, and labelled Serial 2 on the Model 140). The S2 serial port is initially configured for 2400-bps modem support. See "Using a Modem" on page 9-17 for details about using a modem.
2. From the configuration station, establish the modem connection to the IBM 6611 using the directions supplied with the communication package.
3. Log in to the IBM 6611 using the default controlling userid and password.

Default userid: ibm6611c

Default password: ibm6611c

4. Prepare the IBM 6611 to receive the configuration file and use it as the new configuration when it has been received.
 - a. Select **Configuration Files and Reports** from the main menu of the System Manager.
 - b. Select **Import Binary Configuration File** from the next menu.
 - c. Select **modem** as the import method.See "Using the Xmodem Protocol" on page 10-55 for further details about using the Xmodem protocol to transfer files. Figure 14-7 on page 14-13 displays the Configuration Files and Reports menu.
5. Determine the location and name of the configuration file at the configuration workstation. Instruct the configuration workstation to send the configuration file.

If the modem is attached to a different IBM 6611 on the IP network than the IBM 6611 needing to be initially configured, the IBM 6611 has to be minimally configured for

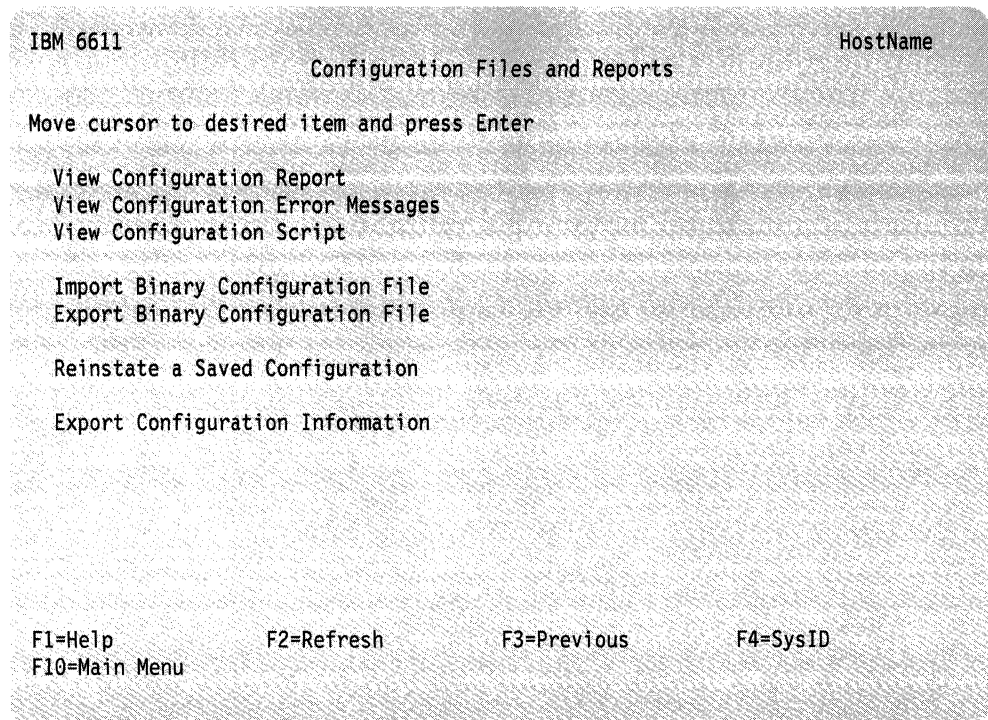


Figure 14-7. Configuration Files and Reports Menu

an IP connection. Perform the following steps to configure the IBM 6611 initially using the modem connection to send the configuration file.

1. Minimally configure the IBM 6611 using the directions provided in “Minimal Configuration Using the System Manager” on page 14-15.
2. From the configuration workstation, establish a modem connection to the IBM 6611 with a modem that is on the same IP network as the IBM 6611 that you minimally configured. See “Using a Modem” on page 9-17 for details about using a modem. Use the directions supplied with the communication package on the configuration workstation for modem connection.
3. Log in to the IBM 6611 with the modem from the configuration workstation. Establish an RLOGIN session from the IBM 6611 with the modem to the IBM 6611 needing to be configured. See “Using Remote Login” on page 9-10 for details about using RLOGIN.
4. Prepare the IBM 6611 that needs to be configured to receive the configuration file and use it as the new configuration when received.
 - a. Select **Configuration Files and Reports** from the main menu of the System Manager.
 - b. Select **Import Binary Configuration File** from the next menu.
 - c. Select **modem** as the import method.

See “Using the Xmodem Protocol” on page 10-55 for further details about using the Xmodem protocol to transfer files. Figure 14-7 displays the Configuration Files and Reports menu.

5. Determine the location and name of the configuration file at the configuration workstation. Instruct the configuration workstation to send the configuration file.

FTP Transfer Method

The configuration file may be sent using FTP, if the configuration workstation is on the IP network and it supports FTP. Use the following steps to configure the IBM 6611 initially using FTP to transfer the file.

1. Minimally configure the IBM 6611 using the directions provided in "Minimal Configuration Using the System Manager" on page 14-15.
2. Know the location and file name of the configuration file on the configuration station. In this procedure, the configuration file name is *config*.
3. From the directory that has the configuration file in the configuration station, use the following scenario to place the configuration file in the transfer directory of the IBM 6611 needing to be configured. What you are expected to input from the configuration station is provided under **Type in**. What you should expect to see displayed on the screen is provided under **Output displayed**.

Type in:

ftp hostname

where *hostname* is the host name of the IBM 6611 needing to be configured. The *IP address* can be used in place of the hostname to identify the IBM 6611 to which the configuration files is sent.

Output displayed:

Connected to hostname.domainname
220 hostname FTP server (Version 4.1 Date) ready.
Name (hostname):

Type in:

6611_userid

Output displayed:

331 Password required for 6611_userid.
Password:

Type in: (Enter the password. It will not be displayed.)

Output displayed:

230 User 6611_userid logged in.
/transfer is read-write and /static is read-only.
ftp>

Type in:

cd /transfer

Output displayed:

250 CWD command successful.
ftp>

Type in:

bi

Output displayed:

200 Type set to I.
ftp>

Type in:

put config

Output displayed:

```
200 PORT command successful.  
150 Opening BINARY mode data connection for filename1.  
226 Transfer complete.  
local: config remote: config  
13029 bytes sent in 0.07388 seconds (172.2 Kbytes/s)  
ftp>
```

Type in:

```
quit
```

Output displayed:

```
221 Goodbye.
```

Note: The numbers associated with the FTP messages are standard message numbers for this protocol. They have no significance other than to identify the message.

4. The configuration file is now in the transfer directory of the IBM 6611. Receive the file and use it as the new configuration:
 - a. Select **Configuration Files and Reports** from the main menu of the System Manager.
 - b. Select **Import Binary Configuration File** from the next menu.
 - c. Select **transfer_directory** as the import method.

A dialog screen appears requesting you to enter the name of the configuration file. The default configuration file name is *config*. If this is not the name of the configuration file that you are importing from the transfer directory, press **F4 (Esc + 4)** to list the files in the transfer directory and select the configuration file from the list. Optionally, you can type the file name in the entry field. Press **Enter** after you have selected or typed the name. Figure 14-7 on page 14-13 shows the Configuration Files and Reports menu.

See “Using the File Transfer Protocol” on page 10-52 for further details about using FTP to transfer files.

Minimal Configuration Using the System Manager

To minimally configure the IBM 6611, you must have either an Ethernet Adapter or a Token-Ring Network 16/4 Adapter configured for IP. The procedure for minimal configuration can be performed by the IBM Customer Engineer (CE), when the IBM 6611 is installed. You need to know the *slot number* and the *IP address* for the adapter. You also need to know the ring speed, if a Token-Ring Network 16/4 Adapter is used. There must be a terminal attached directly to the EIA 232 S1 serial port, that is a supported terminal type or can emulate a supported terminal type. See “Accessing the IBM 6611 through the EIA 232 Serial Ports” on page 9-19 for a list of the supported terminal types.

- Step 1** Log in to the IBM 6611 using this userid, **ibm6611c**, and password, **ibm6611c**. Select the terminal type. See “Logging In to an IBM 6611” on page 9-23 for details about logging in and selecting terminal types.
- Step 2** The main menu of the System Manager is displayed. Select **Adapter and Protocol Configuration** from the System Manager main menu screen. Press **Enter** twice to get to the main Adapter and Protocol Configuration menu. If you are performing the minimal configuration for an Ethernet

Adapter, continue with Step 3. If you are performing the minimum configuration for a Token-Ring Network 16/4 Adapter, go to Step 4.

Step 3 To configure a Ethernet Adapter for IP connection minimally:

1. Select **Set Configuration Values for Single Objects** from the Adapter and Protocol Configuration main menu.
2. Select **Port Level Parameters** from the selector screen.
3. Select the slot number of the Ethernet Adapter from the selector screen.
4. Select **Port 1** from the selector screen.
5. Select **Ethernet Adapter Parameters** from the Configuration Data Type selector screen.
6. A dialog screen appears. Press **Tab** to select **yes** for the Enable interface parameter. Use the defaults of the other parameters. Press **Enter** to update the configuration changes for the Ethernet Adapter.
7. A command status screen is displayed. If the process is successful, a *Command: OK* message is displayed. Press **F3 (Esc + 3)** until you return to the Adapter and Protocol Configuration menu. If you received any error messages, try to correct the problem, or call IBM service personnel for assistance.
8. Go to Step 5.

Step 4 To minimally configure a Token-Ring Network 16/4 Adapter for IP connection:

1. Select **Set Configuration Values for Single Objects** from the Adapter and Protocol Configuration main menu.
2. Select **Port Level Parameters** from the selector screen.
3. Select the slot number of the Token-Ring Network 16/4 Adapter from the selector screen.
4. Select **Port 1** from the selector screen.
5. Select **Token Ring Adapter Parameters** from the Configuration Data Type to Set selector screen.
6. A dialog screen appears. Press **Tab** to select **yes** for the Enable Interface parameter. Press **Tab** to select the correct ring speed for the Token Ring Data Rate parameter. Use the defaults for the other parameters. Press **Enter** to update the configuration changes for the Token-Ring Network 16/4 Adapter.
7. A command status screen is displayed. If the process is successful, a *Command: OK* message is displayed. Press **F3 (Esc + 3)** until you return to the Adapter and Protocol Configuration menu. If you received any error messages, try to correct the problem, or call IBM service personnel for assistance.

Step 5 To configure the correct IP address:

1. Select **Set Configuration Values for Single Objects** from the Adapter and Protocol Configuration main menu.
2. Select **Port Level Parameters** from the selector screen.
3. Select the slot number of the adapter you configured from the selector screen.

4. Select **Port 1** from the selector screen.
5. Select **IP Parameters** from the Configuration Data Type to Set selector screen.
6. A dialog screen is displayed. Enter the IP address of the adapter in the IP Address entry field. Enter the address mask of the IP address in the Subnet Mask entry field. Press **Tab** to select **yes** for the Enable IP routing on this port parameter. Use the defaults for the other parameters. Press **Enter** to add the configuration changes for the IP address.
7. A command status screen is displayed. If the process is successful, a *Command: OK* message is displayed. Press **F3 (Esc + 3)** until you return to the Adapter and Protocol Configuration menu. If you received any error messages, try to correct the problem or call IBM service personnel for assistance.

Step 6 Select **Apply Changes to Configuration Database** from the Adapter and Protocol Configuration menu to apply the configuration changes.

Note: These changes are not dynamic. The IBM 6611 is stopped and restarted. Do not execute any other IBM 6611 tasks until the system has been restarted.

When the IBM 6611 is restarted, it is possible for the Configuration Program to either transfer the configuration file directly to the IBM 6611 or to use FTP to transfer the file to the IBM 6611. See "Direct IP Attachment" on page 14-12 or "FTP Transfer Method" on page 14-14 for further information about initial configuration using the Configuration Program.

Importing and Exporting the Configuration File

Besides initial configuration, there are other situations in which it is necessary for the System Manager to either import the configuration file from the Configuration Program or another IBM 6611 or export the configuration file to the Configuration Program or another IBM 6611. These two tasks can be performed from the Configuration Files and Reports menu. Figure 14-7 on page 14-13 shows the Configuration Files and Reports menu.

Only a controlling user can import the binary configuration file and use it as the current configuration.

To import the configuration file and use it as the current configuration, select **Import Binary Configuration File** from the Configuration Files and Reports menu. A selector screen appears requesting you to select the import method. See Figure 14-8 on page 14-18. Select one of the four methods, depending on the location of the configuration file. After selecting the import method and entering any dialog information, the configuration file is added as the current configuration.

Import method		
Move cursor to desired item and press Enter		
FTP		
modem		
DOS_diskette		
transfer_directory		
F1=Help	F2=Refresh	F3=Previous
F7=Page Up	F8=Page Down	F10=Main Menu

Figure 14-8. Import Method Selector Screen

FTP

Use this method if the configuration file is located in the transfer directory of another IBM 6611 and has the file name *config*. You are required to provide the following input on the dialog screen:

- Host name or IP address of the node containing the configuration file
- Userid configured at that node.

Press **Enter** after typing in the entry fields. You will be prompted for the password of the specified userid.

modem

Use this method if the configuration file is located at a node that is connected to the IBM 6611 over a modem connection.

DOS_diskette

Use this method if the configuration file is located on a DOS diskette that is in the diskette drive of the IBM 6611 and has the file name *config*.

transfer_directory

Use this method if the configuration file is located in the transfer directory of the IBM 6611. It could have been sent to the transfer directory using FTP or Xmodem. The configuration file can have any name. The file name is requested from the dialog screen. The default configuration file name is *config*. If this is not the name of the configuration file that you are importing from the transfer directory, press **F4 (Esc + 4)** to list the files in the transfer directory. Select the configuration file from the list. Optionally, you can type the file name in the entry field. Press **Enter** after you have selected or typed the name.

Select **Export Binary Configuration File** from the Configuration Files and Reports menu to export the configuration file from the IBM 6611 to a remote node, to place the configuration file on a diskette, or to place the configuration file in the transfer directory. A selector screen appears requesting you to select the export method. See Figure 14-9 on page 14-19. Select one of the four methods, depending on the destination of the configuration file. The name of the configuration file is *config*.

Export method		
Move cursor to desired item and press Enter		
FTP modem DOS_diskette transfer_directory		
F1=Help	F2=Refresh	F3=Previous
F7=Page Up	F8=Page Down	F10=Main Menu

Figure 14-9. Export Method Selector Screen

FTP

Use this method to transfer the configuration file to the configuration workstation, if it is a RISC System/6000 workstation, or to another IBM 6611. You are required to provide the following input on the dialog screen:

- Host name or IP address of the node to which the configuration file is being transferred
- Userid configured at that node.

Press **Enter** after typing in each of these entry fields. You will be prompted for the password of the specified userid. If the configuration file is transferred to an IBM RISC System/6000 configuration workstation, it is placed in the home directory for the specified userid. If the configuration file is transferred to another IBM 6611, it is placed in the transfer directory of the IBM 6611. The name of the configuration file is *config*.

modem

Use this method if the configuration file is to be transferred to a configuration workstation that is connected to the IBM 6611 over a modem connection. The name of the configuration file is *config*.

DOS_diskette

Use this method to place the configuration file on a DOS diskette that is in the diskette drive of the IBM 6611. The name of the configuration file is *config*.

transfer_directory

Use this method to place the configuration file in the transfer directory of the IBM 6611. From the transfer directory, it can be transferred out of the IBM 6611 using either FTP or Xmodem. You can name the configuration file any name you want. The file name is requested from the dialog screen. The default configuration file name is *config*. You can also type the file name in the entry field. Press **Enter** after the name is typed.

Reinstating a Saved Configuration File

The IBM 6611 saves the last four configurations that it receives from either the System Manager or the Configuration Program. These configurations can be reinstated from the Configuration Files and Reports menu of the System Manager.

To reinstate a saved configuration file and use it as the current configuration, select **Reinstate a Saved Configuration** from the Configuration Files and Reports menu. A selector screen appears requesting you to select the configuration file to reinstate.

Locate the file you want to reinstate and press **Enter**. Depending on the configuration parameters being changed the IBM 6611 may be restarted.

Working with the Configuration Information Text Files

There are three types of configuration information files, other than the binary configuration file containing the actual configuration information. They are:

- Configuration report
- Configuration error messages
- Configuration script.

Each of these configuration information text files can be viewed with the System Manager or transferred from the IBM 6611 for remote viewing.

Configuration Report

The configuration report contains information about the current configuration. It is provided in both **brief** and **detailed** formats.

The configuration report generated by a user shows the current running configuration unless the user has made some unapplied configuration changes. The configuration report shows all unapplied configuration changes updated by the user who generates the configuration report. It is possible for different users to produce different configuration reports. It is also possible to produce a configuration report that does not accurately reflect the running configuration. To produce a configuration report that accurately reflects the running configuration, either:

- Apply all configuration changes, or
- Reject all uncommitted changes.

The brief configuration report contains a few system level configuration parameters, such as host and domain name. The adapter type in each of the slots is listed along with the protocols configured for that adapter. See Figure 14-11 on page 14-22 for an example of a brief configuration report.

The detailed format contains a complete listing of all the configured configuration objects and the values of each of the parameters. See Figure 14-10 on page 14-21 for an example of a detailed configuration report.

Detailed Configuration Report
IBM 6611 '6611host' on Mon Jul 13 14:10:21 1992
Configuration: UNNAMED CONFIG

Object: Protocol Independent Parameters
(slot 255, port 255, id 21500, count 1, size 100)

IBM 6611 Host Name: 6611host
IBM 6611 Domain name:
Enable name resolution by remotename servers: no
Enable time service by remote time servers: no

Object: List of Controlling User Names and Passwords
(slot 255, port 255, id 22400, count 1, size 20)

User id: ibm6611c
Password: *

Object: List of Viewing User Names and Passwords
(slot 255, port 255, id 22401, count 1, size 20)

User id: ibm6611v
Password: *

Object: IP Parameters
(slot 255, port 255, id 21000, count 1, size 35)

Connection Decay Interval (5 - 20 minutes): 10
Status Of All Defined IP Filters: enable

Object: Ethernet Adapter Parameters
(slot 2, port 1, id 2600, count 1, size 19)

Enable interface: yes
MAC Address: Use card MAC address
Alternate Ethernet MAC Address (Canonical format): 00-00-00-00-00-00
Allow multicasting: no

Object: IP Parameters
(slot 2, port 1, id 1000, count 1, size 52)

IP Address: 9.66.31.8
Subnet mask: 255.255.255.0
Destination IP Address: 0.0.0.0
Maximum transmission unit (bytes): 1500
Enable IP Routing On This Port: yes
Ethernet framing for IP: Both

Figure 14-10. Detailed Configuration Report Example

Brief Configuration Report
IBM 6611 '6611host' on Mon Jul 13 14:09:57 1992

IBM 6611 Host Name: 6611host
IBM 6611 Domain name:
System contact:
System name:
System location:

Slot 1 contains a 6611 X.25 Adapter

Slot 2 contains a 6611 Ethernet Adapter

Configuration data for slot 2, port 1
Ethernet is enabled
IP is enabled
IP Address: 9.66.31.8
Subnet mask: 255.255.255.0

Slot 4 contains a 6611 Token-Ring Adapter

Configuration data for slot 4, port 1
Token-Ring is enabled
IP is enabled
IP Address: 9.66.23.8
Subnet mask: 255.255.255.0

Slot 5 contains a 6611 4-Port SDLC Serial Adapter

Configuration data for slot 5, port 1
Multiport is enabled
Physical link type: EIA232D

Configuration data for slot 5, port 2
Multiport is enabled
Physical link type: EIA232D

Configuration data for slot 5, port 3
Multiport is enabled
Physical link type: EIA232D

Configuration data for slot 5, port 4
Multiport is enabled
Physical link type: EIA232D

Slot 6 contains a 6611 2-Port Serial Adapter

Configuration data for slot 6, port 1
Serial is enabled
Enable Frame Relay On This Port: no
Enable Point to Point Protocol (PPP) On This Port: yes
IP is enabled
IP Address: 8.8.8.2
Subnet mask: 255.255.255.0

Configuration data for slot 6, port 2
Serial is enabled
Enable Frame Relay On This Port: no
Enable Point to Point Protocol (PPP) On This Port: no

Figure 14-11. Brief Configuration Report Example

Configuration Error Message Report

The configuration error messages are placed in a report generated from the error log with all logged configuration errors reported by either the configuration process or the adapters and protocols. Not all configuration errors are sent to the IBM 6611 Error Log. A configuration error report can be generated from those messages that are logged. See "Error Log Facility Overview" on page 11-4 for details about reading an error report. See Figure 14-12 on page 14-23 for an example of an configuration error message report.

```

ERROR LABEL: CONFIG
ERROR ID: 3B3EA22B

Date/Time:      Thu May 28 20:37:19
Sequence Number: 40506
Machine Id:     000268543100
Node Id:        u2
Class:          0
Type:           UNKN
Resource Name:  cfgd

Error Description
CONFIGURATION MISMATCH

Probable Causes
CONFIGURATION
COMMUNICATION CONFIGURATION

User Causes
NO DISKETTE OR DEFECTIVE DISKETTE INSERTED
COMMUNICATION EQUIPMENT POWER OFF

Install Causes
INCORRECT CUSTOMIZATION PARAMETERS
CONFIGURATION ERROR

Failure Causes
SOFTWARE PROGRAM ERROR

Recommended Actions
FOR REMOVABLE MEDIA, CHANGE MEDIA AND RETRY
PLACE BACKUP DISKETTE IN DRIVE
CORRECT CUSTOMIZATION PARAMETERS
CORRECT CONFIGURATION
CONTACT APPROPRIATE SERVICE REPRESENTATIVE

Detail Data
SYMPTOM CODE
92148          cfgd interface-cfgdaemon  372
ERROR CODE
6
PROTOCOL CODE
7
MESSAGE SEVERITY
4
COMMAND
2
CONFIGURATION OBJECT/RECORD
BD6
CONFIGURATION OBJECT/RECORD
BX-TTY-01

```

Figure 14-12. Sample Configuration Error Message Report

Configuration Script

The *configuration script* contains all of the configuration commands issued from the System Manager during the current System Manager session. These commands are in the format:

```
mnppconfig xxxxx
```

where xxxxx is the parameter list for the **mnppconfig** command. The configuration script is useful for debug purposes, or it can be used to build an RSH script to update another IBM 6611 remotely with the same configuration. See Figure 14-13 on page 14-24 for a sample configuration script. See Figure 14-14 on page 14-24 for a sample RSH script created from the configuration script.

```

mnpconfig show object=bx-user-controlling-at
mnpconfig show object=bx-user-viewing-at
mnpconfig add object=bx-user-viewing-at -bx-user-03= 'bat' -bx-user-04= 'man'
mnpconfig add object=bx-user-controlling-at -bx-user-01= 'he' -bx-user-02= 'man'
mnpconfig del object=bx-user-viewing-at -bx-user-03= 'me' -bx-user-04= 'me'
mnpconfig list bx-user-01
mnpconfig list bx-user-03
mnpconfig commit

```

Figure 14-13. Sample Configuration Script

```

# IBM Multiprotocol Network Program
# Script: config_commit
#
# This shell script will update several configuration parameters on a
# IBM 6611. The configuration changes will be applied and committed.
#
# COMMAND SYNTAX:  config_commit
#
# where config_commit is the name of this script.
#
# DEPENDENCIES:  Only a controlling user can update the
#                configuration from an RSH script.
#
# The script has hard coded some variables that need to be changed
# to fit your environment.
#
# IBM 6611 variables:
#   6611h: host name for the IBM 6611
#   6611c: controlling userid at the IBM 6611
#   c:    password of the controlling userid at the IBM 6611
#
# OUTPUT: The given configuration parameters are changed and the
#         configuration committed.
#
rsh 6611h -l 6611c c mnpconfig show object=bx-user-controlling-at
rsh 6611h -l 6611c c mnpconfig show object=bx-user-viewing-at
rsh 6611h -l 6611c c mnpconfig add object=bx-user-viewing-at -bx-user-03= 'bat' -bx-user-04= 'man'
rsh 6611h -l 6611c c mnpconfig add object=bx-user-controlling-at -bx-user-01= 'he' -bx-user-02= 'man'
rsh 6611h -l 6611c c mnpconfig del object=bx-user-viewing-at -bx-user-03= 'me' -bx-user-04= 'me'
rsh 6611h -l 6611c c mnpconfig list bx-user-01
rsh 6611h -l 6611c c mnpconfig list bx-user-03
rsh 6611h -l 6611c c mnpconfig commit

if [ "$?" -eq 0 ]
then
    echo The configuration updates were successfully committed.
    exit 0
else
    echo The configuration updates were not committed.
    exit 1
fi

```

Figure 14-14. Sample RSH Configuration Script

Export Configuration Information

To export the configuration text files using the System Manager:

1. Select **Configuration Files and Reports** from the main menu.
2. Select **Export Configuration Information** on the next menu.
3. Select an Export method from the selector screen.
 - FTP
 - Modem
 - DOS diskette
 - UNIX diskette.
4. With each of these file transfer methods, a selector screen appears requesting the name of the file to be transferred. Select the name of the configuration text file.
 - Transferring files with FTP requires you to give the host name and a userid at the destination node on the dialog screen. You are prompted for the password for the userid.
 - Transferring files to a DOS diskette requires you to give the name of the file on the DOS diskette.
 - Transferring files to a UNIX diskette requires you to specify whether to *append* the file to the end of the diskette or to place it as the only file on the diskette, *create*.

Figure 14-15 shows an example of exporting the brief configuration report using FTP.

```
Enter password for netman
(user enters password invisibly here)
Connected to nv6host.
220 nv6host FTP server (Version 4.1 Sat Nov 23 12:52:09 CST 1991) ready.
331 Password required for netman.
230 User netman logged in.
Local directory is now /tmp/hold/transfer
200 PORT command successful.
150 Opening data connection for config.report.brief.
226 Transfer complete.
748 bytes sent in 0.07346 seconds (9.944 Kbytes/s)
221 Goodbye.
```

Figure 14-15. Example of Export Configuration Information Output Using FTP

Box-Level Single Objects

The following tables list the parameters in the System Manager Configuration Facility and a page reference to the information in other chapters that provide information about how to configure each parameter.

Parameters for AppleTalk

Dialog Item	Reference
Enable AppleTalk	"Enable AppleTalk" on page 3-101

APPN Parameters

Dialog Item	Reference
Network identifier	"Network ID" on page 3-34
Control point name	"Control Point Name" on page 3-34
XID ID number (5 hex digits)	"XID ID Number (Subarea Connection)" on page 3-35
Accept connection requests from any node	"Accept Connection Requests from Any Node" on page 3-35
Maximum number of network nodes in your APPN network	"Maximum Number of Network Nodes in Your APPN Network" on page 3-44
Maximum cached directory entries (10 – 65 535)	"Maximum Cached Directory Entries" on page 3-46
Max. number of end nodes and LEN nodes serviced by this node	"Maximum Number of End Nodes and LEN Nodes Serviced by This Node" on page 3-44
Maximum shared memory (2 - 255 MB)	"Maximum Shared Memory" on page 3-45
Average number of LUs	"Average Number of LUs Associated with End Nodes and LEN Nodes Serviced by This Node" on page 3-44
Enable APPN	"Enable APPN" on page 3-34
Retry Counter	"Retry Counter" on page 14-33

APPN Thresholds

Dialog Item	Reference
Constrained threshold	"Constrained Threshold" on page 14-33
Critical threshold	"Critical Threshold" on page 14-33

Parameters for BGP

Dialog Item	Reference
Enable Border Gateway Protocol – BGP	"Enable Border Gateway Protocol (BGP)" on page 3-67
Default preference (0 – 255)	"Default Preference (0 – 255)" on page 3-68
Default metric (0 – 65 535)	"Default Metric" on page 3-69
Enable BGP Import Filters	"Enable BGP Import Filters" on page 3-77

Protocol Bridging Parameters

Dialog Item	Reference
Enable source route bridging	"Enable Source Route Bridging" on page 3-4
Bridge number (0 – 15)	"Bridge Number" on page 3-4
Designated ring number (hex)	"Designated Ring Number" on page 3-4

Bridging Spanning Tree Parameters

Dialog Item	Reference
Bridge priority (hex)	"Bridge Priority" on page 3-5
Hello time (seconds)	"Hello Time" on page 3-5
Forward delay time (seconds)	"Forward Delay Time" on page 3-5
Maximum age (seconds)	"Maximum Age" on page 3-5

Configuration Process Parameters

Dialog Item	Reference
Hosts that can perform configuration functions on this router	"Hosts that can perform configuration functions on this IBM 6611" on page 4-18
Apply configuration	"Apply Configuration" on page 4-19
Year (1991 – 9999)	"Year" on page 4-19
Month (1 – 12)	"Month" on page 4-19
Day (1 – 31)	"Day" on page 4-19
Hour (0 – 23)	"Hour" on page 4-20
Minute (0 – 59)	"Minute" on page 4-20

DECnet Parameters

Dialog Item	Reference
Enable DECnet router	"Enable DECnet Router" on page 3-116
Local DECnet address (1 – 63, 1 – 1023)	"Local DECnet Address" on page 3-116
Node type	"Node Type" on page 3-116
Area maximum cost (1 – 1022)	"Area Maximum Cost" on page 3-117
Area maximum hops (1 – 30)	"Area Maximum Hops" on page 3-117
Maximum address (1 – 1023)	"Maximum Address" on page 3-118
Maximum area (1 – 63)	"Maximum Area" on page 3-118
Maximum cost (1 – 1022)	"Maximum Cost" on page 3-117
Maximum hops (1 – 30)	"Maximum Hops" on page 3-117
Maximum visits (1 – 63)	"Maximum Visits" on page 3-118
Maximum broadcast non-routers (1 – 1022)	"Maximum Broadcast Non-Routers" on page 3-119
Maximum broadcast routers (1 – 1022)	"Maximum Broadcast Routers" on page 3-118
Routing buffer size (246 – 1486 bytes)	"Routing Buffer Size" on page 3-119

Data Link Switching Parameters

Dialog Item	Reference
Enable forwarding of SNA traffic	"Enable Forwarding of SNA Traffic" on page 3-25
Enable NetBIOS frame forwarding	"Enable NetBIOS Frame Forwarding" on page 3-25
Virtual ring segment number (hex)	"Virtual Ring Segment Number" on page 3-25
Accept connections only from participating DLS routers	"Accept Connections Only from Specific IBM 6611s" on page 3-26
Destination cache timeout (minutes)	"Destination Cache Timeout" on page 3-25
Default DLS IP address for this 6611	"IP Address of Remote IBM 6611" on page 3-26

Parameters for EGP

Dialog Item	Reference
Enable Exterior Gateway Protocol (EGP)	"Enable Exterior Gateway Protocol (EGP)" on page 3-83
Preference (0 – 255)	"Preference" on page 3-83
Maximum initial packet size (1024 – 65535 bytes)	"Maximum Initial Packet Size" on page 3-83
Local autonomous system number (1 – 65534)	"Local Autonomous System Number" on page 3-83
Generate default route	"Generate Default Route" on page 3-83
Enable EGP import filters	"Enable EGP Import Filters" on page 3-88
Default metric (0 – 255)	"Default Metric" on page 3-84

Hello Parameters

Dialog Item	Reference
Enable Hello Protocol	"Enable Hello Protocol" on page 3-63
Broadcast	"Broadcast" on page 3-63
Route preference (0 – 255)	"Route Preference" on page 3-63

IP Parameters

Dialog Item	Reference
Connection decay interval (1 – 20 minutes)	"Connection Decay Interval" on page 3-100
Status of all defined IP filters	"Status of All Defined IP Filters" on page 3-92

IPX Parameters

Dialog Item	Reference
Enable IPX router	"Enable IPX Router" on page 3-102
Split horizon for RIP Filters	"Split Horizon for RIP Filters" on page 3-102
Inbound Filtering mode	"Filtering Mode" on page 3-106
Outbound Filtering Mode	"Filtering Mode" on page 3-107
Router Filtering Mode	"Filtering Mode" on page 3-104
Status of all defined SAP filters	"Status of All Defined SAP Filters" on page 3-102
Status of all defined inbound RIP filters	"Status of All Defined Inbound RIP Filters" on page 3-106
Status of all defined outbound RIP filters	"Status of All Defined Outbound RIP Filters" on page 3-107
Status of all defined RIP router filters	"Status of All Defined RIP Router Filters" on page 3-104
SAP Filtering mode	"Filtering Mode" on page 3-103

Software Lock Parameters

Dialog Item	Reference
Lock value	"Lock Value" on page 4-5

NetBIOS Filter Parameters

Dialog Item	Reference
Destination name filter type	"Destination Name Filter Type" on page 3-49
Source name filter type	"Source Name Filter Type" on page 3-48
Status of all defined destination name filters	"Status of All Defined NetBIOS Destination Name Filters" on page 3-49
Status of all defined source name filters	"Status of All Defined NetBIOS Source Name Filters" on page 3-48

OSPF Parameters

Dialog Item	Reference
Enable OSPF	"Enable OSPF" on page 3-51
Router ID	"Router ID" on page 3-51

Protocol – Independent Parameters

Dialog Item	Reference
IBM 6611 host name	"IBM 6611 Host Name" on page 4-3
Domain name	"Domain Name" on page 4-3
Enable name resolution by remote name servers	"Enable Name Resolution by Remote Name Servers" on page 4-22
Enable time service by remote time servers	"Enable Time Service by Remote Time Servers" on page 4-23

RIP Parameters

Dialog Item	Reference
Enable Routing Information Protocol (RIP)	"Enable Routing Information Protocol (RIP)" on page 3-58
Broadcast	"Broadcast" on page 3-58
Zero reserved fields	"Zero Reserved Fields" on page 3-58
Route preference (0 – 255)	"Route Preference" on page 3-59

SNA Frame Filter Parameters

Dialog Item	Reference
Source frame filter type	"Source Frame Filter Type" on page 3-28
Destination frame filter type	"Destination Frame Filter Type" on page 3-30
Status of all defined SNA source frame filters	"Status of All Defined SNA Source Frame Filters" on page 3-27
Status of all defined SNA destination frame filters	"Status of All Defined SNA Destination Frame Filters" on page 3-29

SNMP System Contact

Dialog Item	Reference
System contact	"System Contact" on page 4-7

SNMP System Name

Dialog Item	Reference
System name	"System Name" on page 4-7

SNMP System Location

Dialog Item	Reference
System location	"System Location" on page 4-7

SNMP Parameters

Dialog Item	Reference
Enterprise specific trap throttle time (0 – 3600 seconds)	"Enterprise-Specific Trap Throttle Time" on page 4-8
Router serial number – prefix	"Router Serial Number Prefix" on page 4-8
Router serial number – suffix	"Router Serial Number Suffix" on page 4-9
Enable SNMP	"Enable SNMP" on page 4-6

Serial Line TTY Parameters

Dialog Item	Reference
Baud rate for S1 serial port (bps)	"Baud Rate for S1 Serial Port" on page 4-4
Baud rate for S2 serial port (bps)	"Baud Rate for S2 Serial Port" on page 4-4

XNS Parameters

Dialog Item	Reference
Enable XNS router	"Enable XNS Router" on page 3-109
Split horizon	"Split Horizon For RIP Filters" on page 3-109
Inbound filtering mode	"Filtering Mode" on page 3-110
Outbound filtering mode	"Filtering Mode" on page 3-111
Router filtering mode	"Filtering Mode" on page 3-112
Status of all inbound RIP filters	"Status of All Inbound RIP Filters" on page 3-109
Status of all outbound RIP filters	"Status of All Outbound RIP Filters" on page 3-111
Status of all RIP router filters	"Status of All RIP Router Filters" on page 3-112

Transparent Bridging Parameters

Dialog Item	Reference
Enable Transparent Bridging	"Enable Transparent Bridging" on page 3-11
Form of MAC addresses	"Form of MAC Addresses" on page 3-11
LLC duplicate address check	"LLC Duplicate Address Check" on page 3-11
Source SAP filter (1 – 4)	"Source SAP Filter" on page 3-14
Ethernet type filter (1 – 4)	"Ethernet Type Value" on page 6-36
MAC address filter (1 – 4)	"MAC Address Filter" on page 6-40
Sliding window filter (1 – 4)	"Sliding Window Filter" on page 6-40

Transparent Bridging Spanning Tree Parameters

Dialog Item	Reference
Bridge priority (4 hex digits)	"Bridge Priority" on page 3-16
Max age (seconds)	"Max Age" on page 3-17
Hello time (seconds)	"Hello Time" on page 3-16
Forward delay (seconds)	"Forward Delay" on page 3-16

Transparent Bridging Destination Values

Dialog Item	Reference
Static destination MAC address. (12 hex digits)	"Static Destination MAC Address" on page 3-13

XNS Static Route Tables Parameters

Dialog Item	Reference
Destination network number (1 – 4294967294)	"Destination Network Number" on page 3-114
Destination network number mask (1 – 4294967294)	"Destination Network Number Mask" on page 3-114
Network number of next hop router (1 – 4294967294)	"Network Number of Next Hop Router" on page 3-114
Next hop router host address (12 hex)	"Next Hop Router Host Address" on page 3-114

APPN Parameters for Threshold (Accessed from System Manager-ONLY)

Constrained Threshold

Required: No

Description: This parameter sets a threshold at which APPN begins to limit any new usage of shared memory allocated to the node.

Dependencies: The percentage specified for this parameter should be less than the percentage specified for the Critical threshold parameter.

Valid Values: 0 to 100 percent. If 0 is specified, APPN uses the default value.

Default Value: 80 percent

Critical Threshold

Required: No

Description: This parameter sets a threshold at which APPN begins to reduce the existing usage of shared memory allocated to the node. For example, the APPN node will establish a window size of one to restrict the flow of messages from connection partners.

Dependencies: The percentage specified for this parameter should be greater than the percentage specified for the Constrained threshold parameter.

Valid Values: 0 to 100 percent. If 0 is specified, APPN uses the default value.

Default Value: 90 percent

Retry Counter

Required: No

Description: This parameter specifies the number of times the APPN network node attempts to restart node processes after a failure has occurred.

Dependencies: None

Valid Values: 0 to 255

Default Value: 3

Port-Level Single Objects

AppleTalk DLCI Available on a Port

Dialog Item	Reference
DLCI number	"DLCI Number" on page 6-64

AppleTalk Port Values

Dialog Item	Reference
Enable AppleTalk on this port	"Enable AppleTalk Routing on This Port" on page 6-60
Port list	"Port Type" on page 6-60
Network number range start (1 – 65 279)	"Network Number Range" on page 6-60
Network number range end (1 – 65 279)	"Network Number Range" on page 6-60
Default zone name (maximum 32 characters)	"Default Zone Name" on page 6-61
Starting value for node ID acquisition (1 – 253)	"Starting Value for Node ID Acquisition" on page 6-61
Enable security filters	"Enable Security Filters" on page 6-62
Enable network number range filter	"Enable Network Number Range Filter" on page 6-63
Accept routing information	"Accept Routing Information" on page 6-64

Source Route Bridging Parameters

Dialog Item	Reference
Enable source route bridging on this port	"Enable Source Route Bridging on This Port" on page 6-5
Ring number (hex)	"Ring Number" on page 6-5
Spanning tree mode	"Spanning Tree Mode" on page 6-6
Enable forwarding of spanning tree packets	"Enable Forwarding of Spanning Tree Explorer Packets" on page 6-7
Path cost (0 – 65 535)	"Path Cost" on page 6-6
Maximum transmission unit (bytes)	"Maximum Transmission Unit" on page 6-5
Hop count filter frame type	"Frame Type" on page 6-28
Hop count	"Hop Count" on page 6-27
Inbound source SAP filter type	"Filter Type" on page 6-9
Inbound source SAP frame type	"Frame Type" on page 6-9
Inbound ring number filter type	"Filter Type" on page 6-12
Inbound ring number frame type	"Frame Type" on page 6-13
Inbound MAC address filter type	"Filter Type" on page 6-22
Inbound MAC address frame type	"Frame Type" on page 6-22
Inbound SNAP filter type	"Filter Type" on page 6-12
Outbound ring number filter type	"Filter Type" on page 6-11
Outbound ring number frame type	"Frame Type" on page 6-11
Outbound MAC address filter type	"Filter Type" on page 6-18
Outbound MAC address frame type	"Frame Type" on page 6-19
Outbound SNAP filter type	"Filter Type" on page 6-21
Outbound source SAP filter type	"Filter Type" on page 6-20
Outbound source SAP frame type	"Frame Type" on page 6-20
Status of inbound ring number filters	"Status of All Defined Ring Number Filters on This Port" on page 6-12
Status of inbound MAC address filters	"Status of All Defined Inbound MAC Filters on This Port" on page 6-9
Status of inbound SNAP filters	"Status of All Defined Inbound SNAP Filters on This Port" on page 6-11
Status of outbound ring number filters	"Status of All Defined Outbound Ring Number Filters on This Port" on page 6-22
Status of outbound MAC address filters	"Status of All Defined Outbound MAC Address Filters on This Port" on page 6-18
Status of outbound SNAP filters	"Status of All Defined Outbound SNAP Filters on This Port" on page 6-21
Status of outbound source SAP filters	"Status of All Defined Outbound Source SAP Filters on This Port" on page 6-20

DECnet Parameters

Dialog Item	Reference
Enable DECnet on this interface	"Enable DECnet on This Interface" on page 6-82
Circuit cost (1 – 63)	"Circuit Cost" on page 6-82
Hello timer (1 – 8191 seconds)	"Hello Timer" on page 6-82
Router priority (0 – 127)	"Router Priority" on page 6-83
Routing timer (1 – 65535 seconds)	"Routing Timer" on page 6-83
Maximum routers (1 – 1022)	"Maximum Routers" on page 6-83
Remote DECnet address	"Remote DECnet Address" on page 6-82
Remote DECnet node type	"Remote DECnet Node Type" on page 6-82
Status of all defined DECnet filters on this port	"Status of All Defined DECnet Filters on This Port" on page 6-84

Ethernet Adapter Parameters

Dialog Item	Reference
Enable interface	"Enable Interface" on page 5-6
MAC address	"MAC Address" on page 5-6
Alternate Ethernet MAC address (canonical format)	"Locally Administered Ethernet MAC Address" on page 5-7
Allow multicasting	"Enable Additional Multicast Addresses" on page 5-7

IP Parameters

Dialog Item	Reference
IP address	"IP Address" on page 6-51
Subnet mask	"Subnet Mask" on page 6-51
Destination IP address	"Destination IP Address for X.25" on page 5-47
Maximum transmission unit (bytes)	"Maximum Transmission Unit" on page 6-52
Enable IP routing on this port	"Enable IP Routing on This Port" on page 6-51

IP Filter Parameters

Dialog Item	Reference
IP Filter ID (1 – 100)	"IP Filter ID" on page 3-92
Filter type	"Filter Type" on page 3-93
Permit/Deny traffic	"Permit or Deny Traffic" on page 3-93
Filter IP Address 1	"Filter IP Address 1" on page 3-93
Filter Subnet Mask 1	"Filter Subnet Mask 1" on page 3-93
Filter IP Address 2	"Filter IP Address 2" on page 3-94
Filter Subnet Mask 2	"Filter Subnet Mask 2" on page 3-94

IPX Parameters

Dialog Item	Reference
IPX Network number	"IPX Network Number" on page 6-68
Enable IPX routing on this port	"Enable IPX routing on this port" on page 6-68
Token-ring encapsulation method	"Encapsulation Method" on page 6-68
Ethernet encapsulation method	"Encapsulation Method" on page 6-68
Software loopback active	"Software Loopback Active" on page 6-69
Filtering mode	"Filtering Mode" on page 6-70
Status of all defined IPX filters on this port	"Status of All Defined IPX Filters on This Port" on page 6-69

SDLC Adapter Parameters

Dialog Item	Reference
Enable interface	"Enable Interface" on page 5-22
Physical link type	"Physical Link Type" on page 5-22
Serial encoding	"Serial Encoding" on page 5-23
Request to send	"Request to Send" on page 5-23
Data terminal ready	"Data Terminal Ready" on page 5-24
Data rate select	"Data Rate Select" on page 5-23

Transparent Bridging Port Parameters

Dialog Item	Reference
Enable Transparent Bridging on this port	"Enable Transparent Bridging on This Port" on page 6-29
Maximum transmission unit size	"Maximum Transmission Unit Size" on page 6-33
Inbound MAC address filter type	"Filter Type" on page 6-33
Inbound source SAP filter type	"Filter Type" on page 6-35
Inbound Ethernet filter Type	"Filter Type" on page 6-36
Inbound sliding window filter type	"Filter Type" on page 6-37
Outbound MAC address filter type	"Filter Type" on page 6-41
Outbound source SAP filter type	"Filter Type" on page 6-43
Status of all defined Inbound source SAP filters on this port	"Status of All Defined Inbound Source SAP Filters on This Port" on page 6-35
Status of all defined inbound MAC address filters on this port	"Status of All Defined Inbound MAC Address Filters on This Port" on page 6-33
Status of all defined inbound Ethernet Type filters on this port	"Status of All Defined Inbound Ethernet Type Filters on This Port" on page 6-36
Status of all defined outbound source SAP address filters on this port	"Status of All Defined Outbound Source SAP Filters on This Port" on page 6-43
Status of all defined outbound MAC address filters on this port	"Status of All Defined Outbound MAC Address Filters on This Port" on page 6-41
Status of all defined outbound Ethernet Type filters on this port	"Status of All Defined Outbound Ethernet Type Filters on This Port" on page 6-44
Status of all defined inbound sliding window filters on this port	"Status of All Defined Inbound Sliding Window Filters on This Port" on page 6-37
Outbound Ethernet filter type	"Filter Type" on page 6-44
Source SAP filter (1 – 4)	"Source SAP Filter" on page 6-40
Ethernet Type filter (1 – 4)	"Ethernet Type Filter" on page 6-40
MAC address filter (1 – 4)	"MAC Address Filter" on page 6-40
Sliding window filter (1 – 4)	"Sliding Window Filter" on page 6-40
Status of all defined outbound sliding window filters on this port	"Status of All Defined Outbound Sliding Window Filters on This Port" on page 6-45
Outbound sliding window filter type	"Filter Type" on page 6-45
Source SAP filter (1 – 4)	"Source SAP Filter" on page 6-47
Ethernet Type filter (1 – 4)	"Ethernet Type Filter" on page 6-48
MAC address filter (1 – 4)	"MAC Address Filter" on page 6-48
Sliding window filter (1 – 4)	"Sliding Window Filter" on page 6-48

NetBIOS Packet Forwarding Parameters

Dialog Item	Reference
Forward NetBIOS frames on this port	"Forward NetBIOS Frames on This Port" on page 6-50
Forward NetBIOS datagram and datagram broadcast message on this port	"Forward NetBIOS Datagram and Datagram Broadcast Message on This Port" on page 6-50

EIA 422/449 Serial Adapter or V.35/V.36 Serial Adapter Port Parameters

Dialog Item	Reference
Enable interface	"Enable Interface" on page 5-10
Data link protocol	"Data Link Protocol" on page 5-9
Cylink serial number (0 – 99999999)	"Cylink Serial Number" on page 5-10
Data encoding	"Data Encoding" on page 5-11
Locally administered MAC address	"Locally Administered MAC Address" on page 5-11
Serial line speed (19200 – 1536000 bps)	"Serial Line Speed" on page 5-10

IBM LAN Bridge Parameters

Dialog Item	Reference
Bridge performance counter threshold	"Performance Counter Threshold" on page 5-12
Telecommunications link error threshold	"Telecommunications Link Error Threshold" on page 5-12
Auto reboot on error	"Auto Reboot on Error" on page 5-12
Memory dump on error	"Memory Dump on Error" on page 5-13
Event log drive	"Event Log Drive" on page 5-13
Enable LAN Bridge PPP on this port	"Enable LAN Bridging Protocol on this Port" on page 5-12
Largest frame size (bytes)	"Largest Frame Size" on page 5-13
Enable ring parameter server	"Enable Ring Parameter Server" on page 5-14
Enable ring error monitor	"Enable Ring Error Monitor" on page 5-14
Enable configuration report server	"Enable Configuration Report Saver" on page 5-14
Link password 0	"Link Password 0" on page 5-14
Link password 1	"Link Password 1" on page 5-15
Link password 2	"Link Password 2" on page 5-15
Link password 3	"Link Password 3" on page 5-15

Frame Relay Parameters

Dialog Item	Reference
Enable frame relay on this port	"Enable Frame Relay on This Port" on page 5-19
Polling interval (seconds)	"Polling Interval" on page 5-19
Full enquiry interval (1 – 255)	"Full Enquiry Interval" on page 5-19
LMI option	"LMI Option" on page 5-19
Use inverse ARP to resolve remote protocol addresses	"Use Inverse ARP to Resolve Remote Protocol Addresses" on page 5-20

Point-to-Point Protocol Parameters

Dialog Item	Reference
Enable Point to Point Protocol (PPP) on this port	"Enable Point-to-Point Protocol (PPP) on This Port" on page 5-16
Maximum receive unit (octets)	"Maximum Receive Unit" on page 5-16
Enable link quality monitoring	"Enable Link Quality Monitoring" on page 5-16
Link quality monitoring interval (usec)	"Link Quality Monitoring Interval" on page 5-17

SNA Parameters

Dialog Item	Reference
Enable SNA frame forwarding on this port	"Enable SNA Frame Forwarding on This Port" on page 6-49

Token-Ring Adapter Parameters

Dialog Item	Reference
Enable interface	"Enable Interface" on page 5-3
MAC address	"MAC Address" on page 5-3
Locally administered address (hex)	"Locally Administered Address" on page 5-4
Token ring data rate	"Token-Ring Data Rate" on page 5-5
MAC address format	"MAC Address Format" on page 5-4
Broadcast type	"Broadcast Type" on page 5-5

X.25 Parameters

Dialog Item	Reference
Type of line	"Type of Line" on page 5-32
Enable X.25	"Enable X.25" on page 5-32

X.25 Subscription Parameters

Dialog Item	Reference
Local DTE address (NUA)	"Local DTE Address (NUA)" on page 5-33
Network identifier	"Network Identifier" on page 5-33
Lowest logical channel number (incoming SVC)	"Lowest LCN for Incoming SVCs" on page 5-34
Number of logical channels for incoming SVCs	"Number of Logical Channels for Incoming SVCs" on page 5-35
Lowest logical channel number (2 – way SVC)	"Lowest LCN for Two-Way SVCs" on page 5-34
Number of logical channels (2 – way SVC)	"Number of LCNs for Two-Way SVCs" on page 5-34
Lowest logical channel number (outgoing SVC)	"Lowest LCN for Outgoing SVCs" on page 5-33
Number of logical channels (outgoing SVCs)	"Number of LCNs for Outgoing SVCs" on page 5-33
Lowest logical channel number (PVC)	"Lowest LCN for PVCs" on page 5-35
Maximum number of PVCs	"Number of LCNs for PVCs" on page 5-35
Auto-call unit	"Auto-Call Unit" on page 5-36
Auto-call unit disconnection timeout	"Auto-Call Unit Disconnection Timeout" on page 5-37
CCITT support	"CCITT Support" on page 5-35
Frame window size	"Frame Window Size" on page 5-36
Connection mode	"Connection Mode" on page 5-36
Frame modulo	"Frame Modulo" on page 5-36

X.25 Network Tuning Parameters

Dialog Item	Reference
T24 timer (seconds)	"T24 Timer" on page 5-46
T25 timer (seconds)	"T25 Timer" on page 5-46
Maximum number of reset packets	"Maximum Number of Reset Packets" on page 5-45
Maximum number of clear packets	"Maximum Number of Clear Packets" on page 5-45
T1 Timer (1 – 255)	"T1 Timer" on page 5-45
T4 timer (seconds)	"T4 Timer" on page 5-45
N2 counter (1 – 255)	"N2 Counter" on page 5-45
Startup counter (1 – 255)	"Startup Counter" on page 5-46
Poll timer (10 – 255)	"Level Poll Timer" on page 5-46

X.25 Subscription PVC Default Parameters

Dialog Item	Reference
Receive packet size	"PVC Receive Packet Size" on page 5-37
Transmit packet size	"Transmit Packet Size" on page 5-39
Receive packet window	"PVC Receive Packet Window Size" on page 5-38
Transmit packet window	"PVC Transmit Packet Window Size" on page 5-38
Auto-reset value	"PVC Auto-reset Value" on page 5-38

X.25 Subscription SVC Parameters

Dialog Item	Reference
Receive packet size	"Default SVC Receive Packet Size" on page 5-39
Transmit packet size	"Default SVC Transmit Packet Size" on page 5-40
Receive packet window	"Default SVC Receive Packet Window Size" on page 5-40
Transmit packet window	"Default SVC Transmit Packet Window Size" on page 5-40
Packet size and packet window size negotiation	"Packet Size and Packet Window Size Negotiation" on page 5-42
Allow incoming calls	"Allow Incoming Calls" on page 5-41
Allow outgoing calls	"Allow Outgoing Calls" on page 5-41
Allow fast select	"Allow Fast Select" on page 5-43
Closed user group	"Closed User Group" on page 5-44
Allow reverse charging	"Allow Reverse Charging" on page 5-42
Include calling address in call request packets	"Include Calling Address in Call Request Packets" on page 5-40
Packet size negotiation facility	"Packet Size Negotiation Facility" on page 5-41
Packet window size negotiation facility	"Packet Window Size Negotiation Facility" on page 5-42
Basic format	"Basic Format" on page 5-43
Extended format	"Extended Format" on page 5-43
CUG with OA selection facility - basic format	"CUG with OA Facility (Basic Format)" on page 5-43
CUG with OA selection facility - extended format	"CUG with OA Facility (Extended Format)" on page 5-44
Reverse charging/fast select facility	"Reverse Charging/Fast Select Facility" on page 5-42
Calling address in incoming call packets	"Calling Address in Incoming Call Packets" on page 5-41

XNS Parameters

Dialog Item	Reference
XNS network number	"XNS Network Number" on page 6-75
Enable XNS routing on this port	"Enable XNS Routing on This Port" on page 6-75
Encapsulation method	"Encapsulation Method" on page 6-75
Encapsulation method	"Encapsulation Method" on page 6-76
Error protocol active	"Error Protocol Active" on page 6-76
Number of bytes returned in an error protocol packet	"Number of Bytes Returned in an Error Protocol Packet" on page 6-76
Software loopback active	"Software Loopback Active" on page 6-76
Filtering mode	"Filtering Mode" on page 6-77
Status of all defined XNS filters on this port	"Status of All Defined XNS Filters on This Port" on page 6-77
Destination host address	"Destination Host Address" on page 6-75

Port-Level List Objects

List of AppleTalk Packet Filters

Dialog Item	Reference
Network number range start (1 – 65279)	"Network Number Range" on page 6-60
Network number range end (1 – 65279)	"Network Number Range" on page 6-60

List of Additional AppleTalk Zone Names

Dialog Item	Reference
Additional zone name (max 32 char)	"Additional Zone Name" on page 6-62

List of MAC Input Filters for SRB

Dialog Item	Reference
Source	"Source Frame Address" on page 6-9
Destination	"Destination Frame Address" on page 6-10
Source mask	"Source Frame Address Mask" on page 6-10
Destination mask	"Destination Frame Address Mask" on page 6-10

List of Ring Input Filters for SRB

Dialog Item	Reference
Ring number (hex)	"Ring Number" on page 6-13
Ring number mask (hex)	"Ring Number Mask" on page 6-13

List of SAP Input Filters for SRB

Dialog Item	Reference
Source SAP value (hex)	"Ring Number" on page 6-5

List of SNAP Input Filters for SRB

Dialog Item	Reference
SNAP value (hex)	"SNAP Value" on page 6-12
SNAP value mask (hex)	"SNAP Value Mask" on page 6-12

List of MAC Output Filters for SRB

Dialog Item	Reference
Source	"Source Frame Address" on page 6-19
Destination	"Destination Frame Address" on page 6-19
Source mask	"Source Frame Address Mask" on page 6-19
Destination mask	"Destination Frame Address Mask" on page 6-20

List of Ring Output Filters for SRB

Dialog Item	Reference
Ring number (hex)	"Ring Number" on page 6-23
Ring number mask (hex)	"Ring Number Mask" on page 6-23

List of SAP Output Filters for SRB

Dialog Item	Reference
Source SAP Value (hex)	"Source SAP Value" on page 6-21

List of SNAP Output Filters for SRB

Dialog Item	Reference
SNAP value (hex)	"SNAP Value" on page 6-21
SNAP value mask (hex)	"SNAP Value Mask" on page 6-22

List of Ring Number—DLCI Pairs for SRB

Dialog Item	Reference
DLCI number	"DLCI" on page 6-5
Ring number (hex)	"Ring Number" on page 6-5

List of MAC Input Filters for TB

Dialog Item	Reference
Source (12 hex digits)	"Source MAC Address" on page 6-33
Destination (12 hex digits)	"Destination MAC Address" on page 6-34
Source mask (12 hex digits)	"Source MAC Address Mask" on page 6-34
Destination mask (12 hex digits)	"Destination MAC Address Mask" on page 6-34

List of SAP Input Filters for TB

Dialog Item	Reference
Source SAP value (12 hex digits)	"Source SAP Value" on page 6-35

List of Sliding Window Input Filters for TB

Dialog Item	Reference
Offset into frame (0 – 1513)	"Offset into Frame" on page 6-38
Sliding window contents (hex)	"Sliding Window Contents" on page 6-38
Sliding window mask (hex)	"Sliding Window Mask" on page 6-39
Filter name	"Filter Name" on page 6-38
Offset starting field	"Offset Starting Field" on page 6-38

List of SNAP Input Filters for TB

Dialog Item	Reference
Ethernet Type (4 hex digits)	"Ethernet Type" on page 6-44
Ethernet Type mask (4 hex digits)	"Ethernet Type Mask" on page 6-36

List of Logical Ports Number to DLCI Pairs for TB

Dialog Item	Reference
DLCI number	"DLCI Number" on page 6-31

List of MAC Output Filters for TB

Dialog Item	Reference
Source (12 hex digits)	"Source MAC Address" on page 6-41
Destination (12 hex digits)	"Destination MAC Address" on page 6-42
Source mask (12 hex digits)	"Source MAC Address Mask" on page 6-42
Destination mask (12 hex digits)	"Destination MAC Address Mask" on page 6-42

List of SAP Output Filters for TB

Dialog Item	Reference
Source SAP value (2 hex digits)	"Source SAP Value" on page 6-43

List of Sliding Window Output Filters for TB

Dialog Item	Reference
Offset into frame (0 – 1513)	"Offset into Frame" on page 6-46
Sliding window contents (hex)	"Sliding Window Contents" on page 6-46
Sliding window mask (hex)	"Sliding Window Mask" on page 6-46
Filter name	"Filter Name" on page 6-45
Offset starting field	"Offset Starting Field" on page 6-46

List of SNAP Output Filters for TB

Dialog Item	Reference
Ethernet Type (4 hex digits)	"Ethernet Type" on page 6-44
Ethernet Type mask (4 hex digits)	"Ethernet Type Mask" on page 6-44

List of DECnet Node to DLCI Mappings

Dialog Item	Reference
Remote DECnet address	"Remote DECnet Address" on page 6-84
Remote DECnet node type	"Remote DECnet Node Type" on page 6-84
DLCI number	"DLCI Number" on page 6-83

List of DECnet Packet Filters

Dialog Item	Reference
Filter ID (1 – 100)	"Filter ID" on page 6-84
Direction in which packet is moving	"Direction in Which the Packet Is Moving" on page 6-85

List of Multicast MAC Addresses

Dialog Item	Reference
Multicast MAC address	"Multicast MAC Address" on page 5-8

List of IP Destination Address to DLCI Mappings

Dialog Item	Reference
Destination IP address	"Destination IP Address" on page 6-55
DLCI value	"DLCI Number" on page 6-56

List of IP Parameters for X.25

Dialog Item	Reference
Destination IP address for X.25	"Destination IP Address for X.25" on page 5-47
Virtual circuit type	"Virtual Circuit Type" on page 5-47
Logical channel number	"Logical Channel (PVCs only)" on page 5-47
Remote DTE address	"Remote DTE Address (SVCs only)" on page 5-47
Receive packet size	"Receive Packet Size" on page 5-48
Transmit packet size	"Transmit Packet Size" on page 5-48
Receive packet window size	"Receive Packet Window Size" on page 5-48
Transmit packet window size	"Transmit Packet Window Size" on page 5-48
Closed user group index	"Closed User Group Index" on page 5-49
Closed user group with outgoing access index	"Closed User Group with Outgoing Access Index" on page 5-49
RPOA indices	"RPOA Indices" on page 5-49
User-defined facilities	"User-Defined Facilities" on page 5-48

List of IPX Destination Address to DLCI Mappings

Dialog Item	Reference
Destination IPX address	"IPX Network Number" on page 6-68
DLCI	"DLCI" on page 6-69

List of IPX Filters

Dialog Item	Reference
Filter ID (1 – 10)	"Filter ID" on page 6-70
Filter on transport control	"Filter on Transport Control" on page 6-71
Transport control value (hex)	"Transport Control Value" on page 6-71
Relational compare operator	"Relational Compare Operator" on page 6-71
Filter on packet type	"Filter on Packet Type" on page 6-70
Packet type value (hex)	"Packet Type Value" on page 6-70
Filter based on destination network	"Filter Based on Destination Network" on page 6-71
Destination network value (hex)	"Destination Network Value" on page 6-71
Filter on destination host	"Filter on Destination Host" on page 6-72
Destination host value (hex)	"Destination Host Value" on page 6-72
Filter on destination socket	"Filter on Destination Socket" on page 6-72
Destination socket value (hex)	"Destination Socket Value" on page 6-72
Filter on source network	"Filter on Source Network" on page 6-73
Source network value (hex)	"Source Network Value" on page 6-73
Filter on source host	"Filter on Source Host" on page 6-73
Source host value (hex)	"Source Host Value" on page 6-73
Filter on source socket	"Filter on Source Socket" on page 6-73
Source socket value (hex)	"Source Socket Value" on page 6-74

List of SNA Stations for Adapter

Dialog Item	Reference
Station address (hex)	"Station Address" on page 5-25
Station token-ring source address (hex)	"Station Token-Ring Source Address" on page 5-25
Station token-ring destination address (hex)	"Station Token-Ring Destination Address" on page 5-26
Transmit window count (frames)	"Transmit Window Count" on page 5-28
Retransmit count (1 – 50 frames)	"Retransmit Count" on page 5-27
Retransmit threshold (frames)	"Retransmit Threshold" on page 5-27
Force disconnect timeout (1 – 600 seconds)	"Force Disconnect Timeout" on page 5-29
Maximum I-field size (265 – 30 729 bytes)	"Maximum I-Field Size" on page 5-28
Primary repoll timeout (1 – 250 tenths of seconds)	"Primary Repoll Timeout" on page 5-29
Primary repoll count	"Primary Repoll Count" on page 5-28
Primary repoll threshold (percent)	"Primary Repoll Threshold" on page 5-27
Primary slow list timeout (seconds)	"Primary Slow List Timeout" on page 5-27
Station token ring source SAP	"Station Token-Ring Source SAP" on page 5-25
Station token ring destination SAP	"Station Token-Ring Destination SAP" on page 5-26
Station XID value	"Station XID Value" on page 5-26

List of DLCIs Attached to Frame Relay

Dialog Item	Reference
DLCI assigned to this port	"DLCIs Assigned to This Port" on page 5-20

List of SAP Values

Dialog Item	Reference
SAP value	"SAP Value" on page 6-49

List of X.25 Subscription PVC Parameters

Dialog Item	Reference
Logical channel number	"PVC Logical Channel Number" on page 5-37
Receive packet size	"Receive Packet Size" on page 5-38
Transmit packet size	"Transmit Packet Size" on page 5-39
Receive packet window	"Receive Packet Window Size" on page 5-39
Transmit packet window	"Transmit Packet Window Size" on page 5-39
Auto-reset value	"Autoreset Value" on page 5-39

List of XNS Destination Address to DLCI Mappings

Dialog Item	Reference
Destination XNS address	"Destination XNS Address" on page 6-76
DLCI	"DLCI" on page 6-77

List of XNS Filters

Dialog Item	Reference
Filter ID (1 – 100)	"Filter ID" on page 6-77
Filter based on checksum	"Filter Based on Checksum" on page 6-78
Checksum value (hex)	"Checksum Value" on page 6-78
Filter on transport control	"Filter on Transport Control" on page 6-78
Transport control value (hex)	"Transport Control Value" on page 6-79
Relational compare operator	"Relational Compare Operator" on page 6-79
Filter on packet type	"Filter on Packet Type" on page 6-78
Packet type value (hex)	"Packet Type Value" on page 6-78
Filter based on destination network	"Filter Based on Destination Network" on page 6-79
Destination network value (hex)	"Destination Network Value" on page 6-79
Filter on destination host	"Filter on Destination Host" on page 6-79
Destination host value (hex)	"Destination Host Value" on page 6-80
Filter on destination socket	"Filter on Destination Socket" on page 6-80
Destination socket value (hex)	"Destination Socket Value" on page 6-80
Filter on source network	"Filter on Source Network" on page 6-80
Source network value (hex)	"Source Network Value" on page 6-80
Filter on source host	"Filter on Source Host" on page 6-81
Source host value (hex)	"Source Host Value" on page 6-81
Filter on source socket	"Filter on Source Socket" on page 6-81
Source socket value (hex)	"Source Socket Value" on page 6-81

Box Level List Objects

List of Valid Configuration Hosts

Dialog Item	Reference
IP address of configuration host	"IP Address" on page 4-18
Address mask	"Address Mask" on page 4-18

List of DECnet Packet Filters

Dialog Item	Reference
Filter ID (1 – 100)	"Filter ID" on page 3-120
Filter type	"Filter Type" on page 3-120
Permit/deny traffic	"Permit or Deny Traffic" on page 3-120
Filter DECnet address 1	"Filter DECnet Address 1" on page 3-120
Filter mask 1	"Filter Mask 1" on page 3-121
Filter DECnet address 2	"Filter DECnet Address 2" on page 3-121
Filter mask 2	"Filter Mask 2" on page 3-121

List of Participating DLS Routers

Dialog Item	Reference
IP address of remote 6611 router	"IP Address of Remote IBM 6611" on page 3-26

List of GATED Export Parameters

Dialog Item	Reference
Export selection name	"Export Selection Name" on page 3-95
Source protocol	"From Protocol" on page 3-95
Destination protocol	"To Protocol" on page 3-99
Destination	"Export destination" on page 3-95
Destination mask	"Destination Mask" on page 3-95
Metric	"Metric" on page 3-96
Restrict	"Restrict" on page 3-96
Source AS number	"AS Number" on page 3-99
Type (1 – 2)	"Type" on page 3-99
Tag (1 – 65536)	"Tag" on page 3-99
Destination AS number	"AS Number" on page 3-95

List of No-HELLO-In/No-HELLO-Out Settings

Dialog Item	Reference
IP address of local interface	"IP Address of Local Interface" on page 3-64
Listen for Hello updates	"Listen for Hello Updates" on page 3-64
Send Hello updates	"Send Hello Updates" on page 3-64

List of Hello Source Routers

Dialog Item	Reference
IP address of source router	"IP Address of Source Router" on page 3-64

List of Hello Trusted Routers

Dialog Item	Reference
IP address of trusted router	"IP Address of Trusted Router" on page 3-64

List of IP Packet Filters

Dialog Item	Reference
Filter IP address 1	"Filter IP Address 1" on page 3-93
Filter subnet mask 1	"Filter Subnet Mask 1" on page 3-93
Filter IP address 2	"Filter IP Address 2" on page 3-94
Filter subnet mask 2	"Filter Subnet Mask 2" on page 3-94
Filter ID (1 – 100)	"IP Filter ID" on page 3-92
Filter type	"Filter Type" on page 3-93
Permit/deny traffic	"Permit or Deny Traffic" on page 3-93

List of IP Static Routes

Dialog Item	Reference
Destination Address IP address	"Destination Address" on page 3-90
Destination mask	"Destination Mask" on page 3-90
Next hop router number 1	"Next Hop Router #1" on page 3-90
Preference (0 – 255)	"Preference" on page 3-91
Retain route in Master table	"Retain Route in Master Table" on page 3-91
Next hop router number 2	"Next Hop Router #2" on page 3-91
Next hop router number 3	"Next Hop Router #3" on page 3-91

List of Inbound IPX RIP Filter Parameters

Dialog Item	Reference
Local IPX interfaces to filter on	"Local IPX Network to Filter on" on page 3-106
Network numbers to filter on	"Network Numbers to Filter on" on page 3-107
Network number (hex)	"Network Number" on page 3-107
Filter ID (1 – 128)	"Filter ID" on page 3-106

List of Outbound IPX RIP Filter Parameters

Dialog Item	Reference
Local IPX interfaces to filter on	"Local IPX Network to Filter on" on page 3-108
Network numbers to filter on	"Network Numbers to Filter on" on page 3-108
Network number (hex)	"Network Number" on page 3-108
Filter ID (1 – 128)	"Filter ID" on page 3-108

List of IPX Router Filters

Dialog Item	Reference
Filter ID (1 – 128)	"Filter ID" on page 3-105
Network numbers to filter on	"Network Numbers to Filter on" on page 3-105
Network number (hex)	"Network Number" on page 3-105
Host address to filter on	"Host Address to Filter on" on page 3-105
Host address (hex)	"Host Address" on page 3-105

List of IPX SAP Filters

Dialog Item	Reference
Server name	"Server Name" on page 3-104
Name	"Name" on page 3-104
Server type	"Server Type" on page 3-103
Type (hex)	"Type" on page 3-103
Server number type	"Network Number" on page 3-103
IPX network number	"Network" on page 3-104
Filter ID (1 – 128)	"Filter ID" on page 3-103

List of NetBIOS Default Destinations

Dialog Item	Reference
Destination name	"Destination Name" on page 3-47
IP address of destination router	"IP Address of Destination Router" on page 3-47

List of NetBIOS Destination Name Filters

Dialog Item	Reference
NetBIOS destination name	"Destination Name" on page 3-50

List of NetBIOS Source Name Filters

Dialog Item	Reference
Source name	"Source Name" on page 3-48

List of Static Host to Internet Address Mappings

Dialog Item	Reference
IP address of host	"IP Address of Host" on page 4-21
Host name	"Host Name" on page 4-21

List of No-RIP-In/No-RIP-Out Settings

Dialog Item	Reference
IP address of local interface	"IP Address of Local Interface" on page 3-59
Listen for RIP updates	"Listen for RIP Updates" on page 3-59
Send RIP updates	"Send RIP Updates" on page 3-60

List of RIP Source Routers

Dialog Item	Reference
IP address of source router	"IP Address of Source Router" on page 3-59

List of RIP Trusted Routers

Dialog Item	Reference
IP address of trusted router	"IP Address of Trusted Router" on page 3-60

List of Remote Name Servers

Dialog Item	Reference
IP address of name server	"IP Address of Name Server" on page 4-22

List of Remote Time Servers

Dialog Item	Reference
IP address of remote time server	"IP Address of Remote Time Server" on page 4-23

List of SNA Default Destinations

Dialog Item	Reference
IP address of destination router	"IP Address of Destination Router" on page 3-27
Destination MAC address	"Destination MAC Address" on page 3-27

List of SNA Destination Frame Filters

Dialog Item	Reference
Source address (hex)	"Source Address" on page 3-30
Source address mask (hex)	"Source Address Mask" on page 3-30
Destination address (hex)	"Destination Address" on page 3-31
Destination address mask (hex)	"Destination Address Mask" on page 3-31
Filter ID (1 – 100)	"Filter ID" on page 3-30

List of SNA Source Frame Filters

Dialog Item	Reference
Source address (hex)	"Source Address" on page 3-28
Source address mask (hex)	"Source Address Mask" on page 3-29
Destination address (hex)	"Destination Address" on page 3-29
Destination address mask (hex)	"Destination Address Mask" on page 3-29
Filter ID (1 – 100)	"Filter ID" on page 3-28

List of SNMP Clients for Traps

Dialog Item	Reference
Trap address (IP address or Domain name)	"Trap Address (IP Address or Domain Name)" on page 4-10
Enable coldstart trap	"Enable coldStart Trap" on page 4-10
Enable warmstart trap	"Enable warmStart Trap" on page 4-10
Enable linkDown trap	"Enable linkDown Trap" on page 4-11
Enable linkUp trap	"Enable linkUp Trap" on page 4-11
Enable authenticationFailure trap	"Enable authenticationFailure Trap" on page 4-11
Enable egpNeighborLoss trap	"Enable egpNeighborLoss Trap" on page 4-12
Enable enterpriseSpecific trap	"Enable enterpriseSpecific Trap" on page 4-12
Trap community name	"Trap Community Name" on page 4-10

List of SNMP Communities

Dialog Item	Reference
Community address (IP address or Domain name)	"Community Address (IP Address or Domain Name)" on page 4-14
Community address mask	"Community Address Mask" on page 4-14
Community access	"Community Access" on page 4-15
Community name	"Community Name" on page 4-14
Community view name	"Community View Name" on page 4-15

List of Controlling User Names and Passwords

Dialog Item	Reference
Userid	"Controlling Userid" on page 4-16
Password	"Controlling Password" on page 4-16

List of Viewing User Names and Passwords

Dialog Item	Reference
Userid	"Viewing Userid" on page 4-16
Password	"Viewing Password" on page 4-17

List of XNS RIP Inbound Filters

Dialog Item	Reference
Local XNS interfaces to filter on	"Local XNS Network to Filter on" on page 3-110
Network numbers to filter on	"Network Numbers to Filter on" on page 3-110
Network number (hex)	"Network Number" on page 3-110
Filter ID (1 – 128)	"Filter ID" on page 3-110

List of XNS RIP Outbound Filters

Dialog Item	Reference
Local XNS interfaces to filter on	"Local XNS Network to Filter on" on page 3-111
Network numbers to filter on	"Network Numbers to Filter on" on page 3-112
Network number (hex)	"Network Number" on page 3-112
Filter ID (1 – 128)	"Filter ID" on page 3-111

List of XNS RIP Router Filters

Dialog Item	Reference
Filter ID (1 – 128)	"Filter ID" on page 3-113
Network numbers to filter on	"Network Numbers to Filter on" on page 3-113
Network number (hex)	"Network Number" on page 3-113
Host address to filter on	"Host Address to Filter on" on page 3-113
Host address (hex)	"Host Address" on page 3-113

List of Transparent Bridging Filters

Dialog Item	Reference
Aging time (10 – 1000000 seconds)	"Aging Time" on page 3-12
Overflow policy	"Overflow Policy" on page 3-12

Appendix A. Configuration Planning Worksheets

These worksheets should be used along with the information in Chapter 3 through Chapter 6 before using the Configuration Program. The worksheets are divided into four parts:

- System Configuration
- System Management Configuration
- Adapter Configuration
- Port-Level Protocol Configuration.

Chapter 3 through Chapter 6 can help you determine what to record on the worksheets. If two of the same adapters or protocols are configured on the same IBM 6611, make copies of the worksheets.

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page ____ of ____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Configuration

Bridging

Source Route Bridge

Enable source route bridging: ☐ Enable ☐ Disable†

Bridge number (0-15): _____

Designated ring number (hex) (R): _____

Port Filter Order

Hop count filter (1-6) _____

Source SAP filter (1-6) _____

SNAP value filter (1-6) _____

Ring number filter (1-6) _____

MAC address filter (1-6) _____

Sliding window filter (1-6) _____

Spanning Tree Parameters

Bridge priority (hex): _____

Hello time (seconds): _____

Forward delay time (seconds): _____

Maximum age (seconds): _____

Data Link Switching

Data Link Switching

Enable forwarding of SNA traffic: ☐ Enable ☐ Disable†

Enable NetBIOS frame forwarding: ☐ Enable ☐ Disable†

DLS

Protocols forwarded via DLS:

SNA ☐ Enable ☐ Disable†

NetBIOS ☐ Enable ☐ Disable†

DLS Specific Parameters

Virtual ring segment number (hex):

Destination cache timeout (minutes):

Default DLS IP address for this 6611:

Accept connections only from participating DLS routers:

☐ Enable ☐ Disable†

List of DLS Partners

IP address of remote 6611 router (R):

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Configuration

NetBIOS

List of NetBIOS Default Destinations

Destination name (R):

IP address of destination router (R):

Destination Name Filters

Status of all defined destination name filters:

☐ Enable† ☐ Disable

Destination name filter type: ☐ Deny ☐ Permit†

List of NetBIOS Destination Name Filters

Destination name (R):

Source Name Filters

Status of all defined source name filters:

☐ Enable† ☐ Disable

Source name filter type: ☐ Deny ☐ Permit†

List of NetBIOS Name Filters

Source name (R):

Destination address (hex):

Destination address mask (hex):

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page ____ of ____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Configuration

Transparent Bridge

Enable transparent bridging: ☐ Enable ☐ Disable†
Form of MAC addresses: ☐ Canonical† ☐ Non-canonical
LLC duplicate address check: ☐ Filter ☐ Forward†

Filtering Database Parameters

Overflow policy: ☐ Learn† ☐ Don't Learn
Aging time (seconds): _____

Static destination address filters:

Port Filter Order

Source SAP filter (1-4): _____
Ethernet Type filter (1-4): _____
MAC address filter (1-4): _____
Sliding window filter (1-4): _____

Spanning Tree Parameters

Bridge priority (hex): _____
Hello time (seconds): _____
Forward delay time (seconds): _____
Maximum age (seconds): _____

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Configuration

Routing—OSPF

OSPF

Enable OSPF: ☐ Enable ☐ Disable

Router ID: _____

List of OSPF Areas

Area ID: _____

Area type: ☐ Transit† ☐ Stub

Stub cost (1-65535): _____

Authentication type: ☐ None† ☐ Simple

List of OSPF Interfaces

Interface IP address (R): _____

Interface type: ☐ Broadcast† ☐ Non-broadcast

Authorization Key: _____

Router priority (0-255): _____

Cost (1-65535): _____

Poll interval (1-255): _____

Retransmit interval (1-3600 seconds): _____

Interface transmit delay (1-3600 seconds): _____

Router dead interval (1-65535 seconds): _____

Hello interval (1-255 seconds): _____

List of OSPF Neighbors

IP address of neighbor router (R): _____

Eligible to become designated router: ☐ Enable ☐ Disable†

List of Network Ranges

Network number (R): _____

Network mask (R): _____

List of Virtual Links

Virtual link ID (R): _____

Virtual neighbor ID (R): _____

Transit area ID (R): _____

Authorization key: _____

Retransmit interval (1-3600 seconds): _____

Interface transit delay (1-3600 seconds): _____

Router dead interval (1-65535 seconds): _____

Hello interval (1-255 seconds): _____

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Configuration

Routing—RIP

Enable routing information protocol (RIP): ☐ Enable
☐ Disable†

Broadcast: ☐ Enable† ☐ Disable

Zero reserved fields: ☐ Enable† ☐ Disable

Route preference (0-255): _____

List of RIP Source Routers

IP address of source router (R):

List of RIP Interface Settings

IP address of local interface (R):

Listen for RIP updates: ☐ Enable† ☐ Disable

Send RIP updates: ☐ Enable† ☐ Disable

List of RIP Trusted Routers

IP address of trusted router (R):

List of Imports

Name of import filter (R):

List of Destinations

Destination (R):

Destination mask:

Preference (0-255): _____

Restrict: ☐ Enable ☐ Disable†

Filter routes from:

- ☐ All sources†
☐ Remote router
☐ Interface

List of RIP Import Routers

IP address of remote router:

List of RIP Import Interfaces

IP address of local interface:

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Configuration

Routing—Hello

Enable Hello protocol: ☐ Enable ☐ Disable†

Broadcast: ☐ Enable† ☐ Disable

Route preference (0-255): _____

List of Source Routers

IP address of source router (R):

List of Hello Interface Settings

IP address of local interface (R):

Listen for Hello updates: ☐ Enable† ☐ Disable

Send Hello updates: ☐ Enable† ☐ Disable

List of Trusted Routers

IP address of trusted router:

List of Imports

Name of import filter (R): _____

List of Destinations

Destination (R):

Destination mask:

Preference (0-255): _____

Restrict routes: ☐ Enable ☐ Disable†

Filter routes from:

☐ All sources†

☐ Remote router

☐ Interface

List of Hello Import Routers

IP address of remote router:

List of Hello Import Interfaces

IP address of local interface:

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Configuration

Routing—BGP

Enable Border Gateway Protocol: ☐ Enable ☐ Disable†

Generate default route: ☐ Enable ☐ Disable†

Local autonomous system number (1-65534)(R): _____

Default preference (0-255): _____

Default metric (0-65535): _____

List of BGP Groups (R)

Autonomous system number-ASN (1-65534)(R):

BGP group type:

☐ External† ☐ Test ☐ Internal ☐ IGP
☐ External† ☐ Test ☐ Internal ☐ IGP
☐ External† ☐ Test ☐ Internal ☐ IGP
☐ External† ☐ Test ☐ Internal ☐ IGP

BGP group name:

Metric out (0-65535):

Next hop destination:

Interface IP address:

Generate default route:

☐ Enable† ☐ Disable
☐ Enable† ☐ Disable
☐ Enable† ☐ Disable
☐ Enable† ☐ Disable

Passive:

☐ Enable ☐ Disable†
☐ Enable ☐ Disable†
☐ Enable ☐ Disable†
☐ Enable ☐ Disable†

Default network in:

☐ Enable ☐ Disable†
☐ Enable ☐ Disable†
☐ Enable ☐ Disable†
☐ Enable ☐ Disable†

Default network out:

☐ Enable ☐ Disable†
☐ Enable ☐ Disable†
☐ Enable ☐ Disable†
☐ Enable ☐ Disable†

Preference (0-255):

Hold time (20-65535):

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Configuration

List of Configured Neighbors

BGP neighbor IP address (R):

BGP neighbor name:

Metric out (0-65535):

Next hop destination:

Interface IP address:

Generate default route:

☐ Enable†	☐ Disable
☐ Enable†	☐ Disable
☐ Enable†	☐ Disable
☐ Enable†	☐ Disable

Passive:

☐ Enable	☐ Disable†
☐ Enable	☐ Disable†
☐ Enable	☐ Disable†
☐ Enable	☐ Disable†

Default network in:

☐ Enable	☐ Disable†
☐ Enable	☐ Disable†
☐ Enable	☐ Disable†
☐ Enable	☐ Disable†

Default network out:

☐ Enable	☐ Disable†
☐ Enable	☐ Disable†
☐ Enable	☐ Disable†
☐ Enable	☐ Disable†

Preference (0-255):

Hold time (20-65535):

List of Unconfigured Neighbors

Neighbor:

☐ All†	☐ Host	☐ Network
☐ All†	☐ Host	☐ Network
☐ All†	☐ Host	☐ Network
☐ All†	☐ Host	☐ Network

BGP neighbor name:

IP address (R):

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Configuration

List of Unconfigured Neighbors (cont.)

Mask:

Preference (0-255):

List of BGP Import Filters

Enable BGP import filters: ☐ Enable ☐ Disable†

Import route filters:

- | | |
|-------------------------------------|----------------------------------|
| ☐ AS number† | ☐ AS path |
| ☐ AS number† | ☐ AS path |
| ☐ AS number† | ☐ AS path |
| ☐ AS number† | ☐ AS path |

BGP import name (R):

Autonomous system number (1-65534)(R):

Autonomous system path specification (R):

AS path origin (R):

- | | | | |
|------------------------------|------------------------------|-------------------------------------|-------------------------------|
| ☐ IGP | ☐ EGP | ☐ Incomplete | ☐ Any† |
| ☐ IGP | ☐ EGP | ☐ Incomplete | ☐ Any† |
| ☐ IGP | ☐ EGP | ☐ Incomplete | ☐ Any† |
| ☐ IGP | ☐ EGP | ☐ Incomplete | ☐ Any† |

Restrict imports:

- | | |
|---------------------------------|-----------------------------------|
| ☐ Enable | ☐ Disable† |
| ☐ Enable | ☐ Disable† |
| ☐ Enable | ☐ Disable† |
| ☐ Enable | ☐ Disable† |

List of BGP Destinations (R)

Destination (R):

Destination mask:

Restrict routes:

- | | |
|---------------------------------|-----------------------------------|
| ☐ Enable | ☐ Disable† |
| ☐ Enable | ☐ Disable† |
| ☐ Enable | ☐ Disable† |
| ☐ Enable | ☐ Disable† |

Preference (0-255):

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page ____ of ____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Configuration

Routing—EGP

Enable Exterior Gateway Protocol: ☐ Enable ☐ Disable†

Local autonomous system number (1-65534): _____

Maximum initial packet size (1024-65535 bytes): _____

Preference (0-255): _____

Generate default route: ☐ Enable ☐ Disable†

Default metric (0-255): _____

List of EGP Groups

EGP group name (R): _____

Neighbor ASN (1-65534): _____

Maximum active neighbors: _____

List of EGP Neighbors

EGP neighbor IP address (R): _____

Generate default routes from this neighbor: ☐ Enable†

☐ Disable

Import default route: ☐ Enable ☐ Disable†

Export default route: ☐ Enable ☐ Disable†

Minimum hello interval (30-900 seconds): _____

Minimum polling interval (120-3600 seconds): _____

Default metric (0-255): _____

Group Options

Preference (0-255): _____

Default metric (0-255): _____

Generate default from this neighbor group: ☐ Enable†

☐ Disable

Import default route: ☐ Enable ☐ Disable†

Export default route: ☐ Enable ☐ Disable†

Minimum hello interval (30-900 seconds): _____

Minimum polling interval (120-3600 seconds): _____

Next hop address or domain name: _____

EGP Imports

Enable EGP import filters: ☐ Enable ☐ Disable†

List of EGP Imports

Autonomous system number (R): _____

Restrict: ☐ Enable ☐ Disable†

Preference (0-255): _____

List of EGP Destinations

Destination (R): _____

Destination mask: _____

Restrict routes: ☐ Enable ☐ Disable†

Preference (0-255): _____

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Configuration

Routing—Static Routes

List of IP Static Routes (Destination—Next Hop)

Destination address (R):

Next hop router (R):

Destination mask:

Preference (0-255): _____

Retain route in master table: ☐ Enable ☐ Disable†

Routing—Packet Filters

Status of all defined IP filters: ☐ Enable† ☐ Disable

List of IP Packet Filters (Filter ID—IP Address 1)

ID filter ID (1-100) (R):

Filter subnet mask 1:

Filter type: ☐ Singular† ☐ Dual

Permit/deny traffic: ☐ Deny ☐ Permit†

Filter IP address 1 (R):

Filter IP address 2:

Filter subnet mask 2:

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page ____ of ____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Configuration



Route Exports

List of Exports

Export selection name (R): _____

OSPFase only

Type (1-2)(R): _____

Source

From protocol (R):

- ☐ EGP†
- ☐ RIP
- ☐ Hello
- ☐ Static
- ☐ Default
- ☐ OSPF
- ☐ OSPFase
- ☐ Direct
- ☐ BGP
- ☐ AS Path

Tag (1-65536): _____

Routing—IP over X.25

Connection decay interval (minutes): _____

Autonomous system path specification (R): _____

AS path origin (R): ☐ IGP ☐ EGP
☐ Incomplete ☐ Any†

AS number: _____

Destination

To protocol (R):

- ☐ RIP†
- ☐ Hello
- ☐ EGP
- ☐ OSPFase
- ☐ BGP

AS number: _____

Destination (R): _____

Destination mask: _____

Metric: _____

Restrict: ☐ Enable ☐ Disable†

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Configuration

Routing—IPX

Enable IPX router: ☐ Enable ☐ Disable†

Split horizon for RIP filters:

☐ On† ☐ Poison reverse ☐ Off

SAP Filters

Status of all defined SAP filters: ☐ Enable† ☐ Disable

Filtering mode: ☐ Deny† ☐ Permit

List of SAP Filters

Filter ID (1-128) (R):

Server type: ☐ All server types† ☐ Enter server type

Type (hex): _____

Network number: ☐ All Networks† ☐ Enter network number

Network (hex): _____

Server name: ☐ All servers† ☐ Enter server name:

Name: _____

Router RIP Filters

Status of all defined RIP router filters: ☐ Enable†
☐ Disable

Filtering mode: ☐ Deny† ☐ Permit

List of RIP Router Filters

Filter ID (1-128) (R):

Network numbers to filter on:

☐ All Networks† ☐ Enter Network Number

List of RIP Router Filters (continued)

Network number (hex): _____

Host address to filter on:

☐ All Hosts† ☐ Enter Host Address

Host address (hex): _____

Inbound RIP Filters

Status of all defined inbound RIP filters: ☐ Enable† ☐ Disable

Filtering mode: ☐ Deny† ☐ Permit

List of Inbound IPX RIP Filters

Filter ID (1-128) (R):

Local IPX network to filter on (R): _____

Network numbers to filter on:

☐ All Networks† ☐ Enter Network Number

Network number (hex): _____

Outbound RIP Filters

Status of all defined outbound RIP filters: ☐ Enable† ☐ Disable

Filtering mode: ☐ Deny† ☐ Permit

List of Outbound IPX RIP Filters

Filter ID (1-128) (R):

Local IPX network to filter on (R): _____

Network numbers to filter on: _____

☐ All networks† ☐ Enter network number

Network number (hex): _____

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page ____ of ____

Complete one worksheet for each IBM 6611 — Name _____ Slot ____ Port ____

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Configuration

Routing—XNS

Enable XNS router: ☐ Enable ☐ Disable†

Split horizon:

☐ On†

☐ Poison reverse

☐ Off

Inbound RIP Filters

Status of all inbound RIP filters: ☐ Enable† ☐ Disable

Filtering mode: ☐ Deny† ☐ Permit

List of Inbound RIP Filters

Filter ID (1-128) (R):

Local XNS network to filter on (R): _____

Network numbers to filter on:

☐ All Networks†

☐ Enter Network Number

Network number (hex): _____

Outbound RIP Filters

Status of all outbound RIP filters: ☐ Enable† ☐ Disable

Filtering mode: ☐ Deny† ☐ Permit

List of Outbound RIP Filters

Filter ID (1-128) (R):

Local XNS network to filter on (R): _____

Routing—XNS (continued)

Network numbers to filter on:

☐ All networks†

☐ Enter network number

Network number (hex): _____

RIP Router Filters

Status of all RIP router filters: ☐ Enable† ☐ Disable

Filtering mode: ☐ Deny† ☐ Permit

List of RIP Router Filters

Filter ID (1-128) (R):

Network numbers to filter on:

☐ All networks†

☐ Enter network number

Network number (hex): _____

Host address to filter on:

☐ All hosts†

☐ Enter host address

Host address (hex): _____

Static Route

Destination Network Number:

Destination Network Number Mask:

Network Number of Next Hop Router:

Next Hop Router Host Address (hex):

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Configuration

AppleTalk

Enable AppleTalk: ☐ Enable ☐ Disable†

Advanced Peer-to-Peer Networking (APPN)

Network Node Configuration

Enable APPN: ☐ Enable ☐ Disable†

Network ID (R): _____

Control Point Name (R): _____

XID ID Number (hex): _____

Accept Connection Requests from any Node: ☐ Yes† ☐ No

Tuning This APPN Network Node

Max number of Network Nodes in your APPN Network (decimal): _____

Max number of End Nodes and LEN Nodes serviced by this Node (decimal): _____

Average number of LUs associated with End Nodes and LEN Nodes serviced by this Node (decimal): _____

Max Cached Directory Entries (decimal): _____

Max Shared Memory (decimal): _____

Address of this Node for Data Link Switching

MAC Address (hex): _____

SAP Address (hex): _____

Adjacent Node Definitions-Data Link Switching

Link Station Name (R): _____

MAC Address (R)(hex): _____

SAP Address (hex): _____

Activate Link Automatically: ☐ Enable† ☐ Disable

Enable Session Level Security: ☐ Enable ☐ Disable†

Key (hex): _____

Adjacent Node Type: ☐ APPN Node† ☐ LEN Node

Fully Qualified Control Point Name: _____

XID Block Number (hex): _____

XID ID Number (hex): _____

Fully Qualified LU Name: _____

Adjacent Node Definitions-IP

Link Station Name (R): _____

IP Address (R): _____

Activate Link Automatically: ☐ Enable† ☐ Disable

Enable Session Level Security: ☐ Enable ☐ Disable†

Key (hex): _____

Fully Qualified Control Point Name: _____

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page ____ of ____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Configuration

Routing—DECnet

Enable DECnet router: ☐ Enable ☐ Disable†

Local DECnet address (1-63.1-1023) (R): _____

Buffer size (246-1486 bytes): _____

Node type: ☐ Routing-IV† ☐ Area

Area maximum hops (1-30): _____

Area maximum cost (1-1022): _____

Maximum hops (1-30): _____

Maximum cost (1-1022): _____

List of DECnet Optional Parameters

Maximum address (1-1023): _____

Maximum area (1-63): _____

Maximum visits (1-63): _____

Maximum Broadcast

Non-routers (1-1022): _____

Routers (1-1022): _____

List of DECnet Filters

Filter ID (1-100) (R): _____

Filter type: ☐ Singular† ☐ Dual

Permit/deny traffic: ☐ Deny ☐ Permit†

Filter DECnet address 1 (R): _____

Filter Mask 1: _____

Filter DECnet address 2: _____

Filter Mask 2: _____

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page ____ of ____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Management

 IBM 6611 host name: _____
Domain name: _____
Baud rate for S1 serial port (bps):
☐ 9600† ☐ 2400 ☐ 1200 ☐ 19200 ☐ 38400
Baud rate for S2 serial port (bps):
☐ 9600† ☐ 2400 ☐ 1200 ☐ 19200 ☐ 38400
Lock value: ☐ Lock ☐ Unlock†

SNMP

Enable SNMP: ☐ Enable ☐ Disable†
System contact (R): _____
System name (R): _____
System location (R): _____
Enterprise specific trap throttle time (0-3600 seconds): _____
Router serial number (nn-nnnnnnn): _____

SNMP Traps

List of Clients Who Can Receive Traps

Trap address (IP address or domain name) (R):

Trap community name (R):

Enable coldstart trap: ☐ Enable† ☐ Disable
Enable warmstart trap: ☐ Enable† ☐ Disable
Enable linkDown trap: ☐ Enable† ☐ Disable
Enable linkUp trap: ☐ Enable† ☐ Disable
Enable authenticationFailure trap: ☐ Enable† ☐ Disable
Enable egpNeighborLoss trap: ☐ Enable† ☐ Disable
Enable enterpriseSpecific trap: ☐ Enable† ☐ Disable

List of SNMP Views

View name (R):

List of SNMP MIB Subtrees

MIB subtree (R):

List of SNMP Communities

Community name (R):

Community address (IP address or domain name):

Community address mask:

Community access: ☐ Read only† ☐ None

Community view name:

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

System Management

Users of IBM 6611

List of Controlling Users of System Manager

Userid: _____

Password: _____

List of Viewing Users of System Manager

Userid: _____

Password: _____

Configuration Hosts

Hosts that can perform configuration functions on this IBM 6611:

- ☐ All hosts†
☐ List of specific hosts

List of Configuration Hosts for this 6611

IP address: _____

Address mask: _____

Time to Perform Configuration

Apply configuration: ☐ Immediately† ☐ At next IML
☐ At a specific time and day

Year (1991-9999): _____

Month (1-12): _____

Day (1-31): _____

Hour (0-23): _____

Minute (0-59): _____

Remote Host Names

List of Remote Host Names to IP Addresses

IP address of host

Host name

Name Servers

Enable name resolution by remote name servers: ☐ Enable
☐ Disable†

List of Remote Name Servers

IP address of name server: _____

Time Servers

Enable time service by remote time servers: ☐ Enable
☐ Disable†

List of Remote Time Servers

IP address of remote time server: _____

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

Adapter Configuration

Token-Ring Network 16/4 Adapter Slot _____

Physical Interface

Enable interface: ☐ Enable† ☐ Disable

MAC address:

☐ Universally administered address†

☐ Locally administered address

Locally administered address (hex): _____

MAC address format: ☐ Non-canonical† ☐ Canonical

Token-ring data rate: ☐ 4 Mbps† ☐ 16 Mbps

Broadcast type: ☐ Non-local† ☐ Local

Ethernet Adapter Slot _____

Physical Interface

Enable interface: ☐ Enable† ☐ Disable

MAC address:

☐ Universally administered address†

☐ Locally administered address

Locally administered address (canonical format): _____

Enable additional multicast addresses:

☐ Enable ☐ Disable†

List of Multicast Addresses

Multicast MAC address (hex):

Go to "Port-Level Protocol Parameters"
to complete the adapter configuration.

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____ Slot _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

EIA 422/449 Serial Adapter or V.35/V.36 Serial Adapter

Point-to-Point Protocol

Physical Interface Port _____
Enable interface: ☐ Enable† ☐ Disable
Cylink serial number (0-99999999): _____
Serial line speed (19200-204800 bps): _____
Data encoding: ☐ NRZI† ☐ NRZ
Local administered MAC address (R): _____

PPP

Enable PPP on this port:
☐ Enable† ☐ Disable
Maximum receive unit (octets): _____
Enable link quality monitoring:
☐ Enable ☐ Disable†
Link quality monitoring interval (usec): _____

Go to "Port-Level Protocol Parameters"
to complete the adapter configuration.

LAN Bridging Protocol

Physical Interface Port _____
Enable Interface: ☐ Enable† ☐ Disable
Cylink serial number (0-99999999): _____
Serial line speed (1920-204800 bps): _____
Locally administered MAC address (R): _____

LAN Bridge Port Defaults

Enable LAN bridge PPP:
☐ Enable† ☐ Disable
Auto reboot on error:
☐ Enable† ☐ Disable
Performance counter threshold (0-9999): _____
Telecommunications link error
threshold (0-9999): _____
Memory dump on error:
☐ Default drive† ☐ A drive ☐ B drive
☐ C drive ☐ D drive
Event log drive:
☐ Default drive† ☐ A drive ☐ B drive
☐ C drive ☐ D drive
Largest frame size:
☐ 516 ☐ 1500 ☐ 2052†

Network Management Parameters

Enable ring parameter server:
☐ Enable† ☐ Disable
Enable ring error monitor:
☐ Enable† ☐ Disable
Enable configuration report server:
☐ Enable† ☐ Disable
Passwords to link to network managers
(up to 4 links):
PW 0: _____ PW 2: _____
PW 1: _____ PW 3: _____

Frame Relay

Physical Interface Port _____
Enable interface: ☐ Enable† ☐ Disable
Cylink serial number (0-99999999): _____
Serial line speed (19200-204800 bps): _____
Data encoding: ☐ NRZI† ☐ NRZ
Local administered MAC address (R): _____

Frame Relay

Enable frame relay on this port:
☐ Enable† ☐ Disable
Polling interval (seconds): _____
Full enquiry interval (1-255): _____
LMI option:
☐ ANSI T1.617 Annex D
☐ LMIRev1
☐ None
Use Inverse ARP to resolve
remote protocol addresses:
☐ Enable† ☐ Disable
List of DLCI Numbers for This Port
DLCIs assigned to this port (R):

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____ Slot _____ Port _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

Adapter Configuration

SDLC Adapter

SDLC Adapter

Physical link type: ☐ EIA232D† ☐ V.35 ☐ X.21

Physical Interfaces

Enable interface: ☐ Enable† ☐ Disable

Serial encoding: ☐ NRZ† ☐ NRZI

Data rate select: ☐ Fault† ☐ Alternate

Request to send: ☐ Continuous† ☐ Controlled

Data terminal ready:

☐ Connect Data Set to Line (CDSTL)†

☐ Data Terminal Ready (DTR)

List of SNA Stations

Station address (hex) (R): _____

Station token-ring source address (hex) (R): _____

Station token-ring source SAP (R): _____

Station token-ring destination address (hex): _____

Station token-ring destination SAP: _____

Station XID value (hex): _____

SNA Station Detail - Page 2

Primary slow list timeout (seconds): _____

Retransmit count (1-50 frames): _____

Retransmit threshold (frames): _____

Primary repoll threshold (percent): _____

Primary repoll count: _____

Transmit window count (frames): _____

Maximum I-field size (265-30729 bytes): _____

Forced disconnect timeout (1-600 seconds): _____

Primary repoll timeout (1-250 tenths of seconds): _____

6611 X.25 Adapter

Enable X.25: ☐ Enable† ☐ Disable

Type of line: ☐ DTE† ☐ Back-to-Back DTE

6611 X.25 Adapter (continued)

Subscription

Local DTE address (NUA) (R): _____

Network identifier:

☐ Datex-P ☐ DDN

☐ Datapac ☐ Other public†

☐ Telenet ☐ Other private

Logical Channel Parameters

Circuit Type	Lowest Number	Number of Channels
SVC outgoing	_____	_____
SVC two-way	_____	_____
SVC incoming	_____	_____
PVC	_____	_____

Subscription Mapping - 2

CCITT Support: ☐ 1980 ☐ 1984†

Frame window size: _____

Frame modulo: ☐ 8† ☐ 128

Connection mode: ☐ Active† ☐ Passive

Auto-Call Options

Auto-call unit: ☐ None†
☐ Outgoing calls
☐ Incoming calls
☐ Two-way calls

Auto-call unit disconnection timeout: _____

PVC Settings

List of PVCs

Logical channel number: _____

Receive packet size:

☐ 64 ☐ 128† ☐ 256 ☐ 512 ☐ 1024 ☐ 2048 ☐ 4096

Transmit packet size:

☐ 64 ☐ 128† ☐ 256 ☐ 512 ☐ 1024 ☐ 2048 ☐ 4096

Receive packet window: _____

Transmit packet window: _____

Autoreset Value: _____

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page ____ of ____

Complete one worksheet for each IBM 6611 — Name _____ Slot ____ Port ____

Note: Defaults are noted using a (†) and required information is noted using an (R).

PVC Settings (continued)

PVC Default Settings

Receive packet size:

☐ 64 ☐ 128† ☐ 256 ☐ 512 ☐ 1024 ☐ 2048 ☐ 4096

Transmit packet size:

☐ 64 ☐ 128† ☐ 256 ☐ 512 ☐ 1024 ☐ 2048 ☐ 4096

Receive packet window: _____

Transmit packet window: _____

Autoreset Value: _____

SVC Defaults

Receive packet size:

☐ 64 ☐ 128† ☐ 256 ☐ 512 ☐ 1024 ☐ 2048 ☐ 4096

Transmit packet size:

☐ 64 ☐ 128† ☐ 256 ☐ 512 ☐ 1024 ☐ 2048 ☐ 4096

Receive packet window: _____

Transmit packet window: _____

Include calling address in call request packets:

☐ Include†

☐ Do not include

Calling address in incoming call packets: _____

Allow incoming calls: ☐ Allow† ☐ Forbid

Allow outgoing calls: ☐ Allow† ☐ Forbid

Facilities Control

Packet size negotiation facility: ☐ Enable† ☐ Disable

Packet window size negotiation facility: ☐ Enable† ☐ Disable

Packet size and packet window size negotiation:

☐ Validate ☐ Negotiate†

Reverse charging/fast select facility: ☐ Enable† ☐ Disable

Allow reverse charging: ☐ Allow† ☐ Forbid

Allow fast select: ☐ Allow† ☐ Forbid

Closed User Group (CUG) Selection Facility

Basic format: ☐ Enable† ☐ Disable

Extended format: ☐ Enable ☐ Disable†

CUG with OA selection facility - basic format:

☐ Enable ☐ Disable†

CUG with OA selection facility - extended format:

☐ Enable ☐ Disable†

Closed user group:

☐ 0 ☐ 1† ☐ 2 ☐ 4 ☐ 8 ☐ 16 ☐ 32 ☐ 64

IP

Enable IP routing on this port: ☐ Enable† ☐ Disable

Subnet mask: _____

IP address (R): _____

Maximum transmission unit (bytes): _____

Network Tuning

N2 counter (1-255): _____

T1 timer (1-255): _____

T4 timer (seconds): _____

Packet Level Tuning

Maximum number of clear packets: _____

Maximum number of reset packets: _____

T24 timer (seconds): _____

T25 timer (seconds): _____

Physical Level Tuning

Startup counter (1-255): _____

Poll timer (10-255): _____

IP/X.25 Mapping

List of X.25 Remote Hosts

Destination IP address for X.25 (R): _____

Virtual circuit type: ☐ SVC† ☐ PVC

Logical channel number (PVC only) (R): _____

Remote DTE address (SVC opnly) (R): _____

Optional Questions (SVC Parameters)

Receive packet size:

☐ 64 ☐ 128 ☐ 256 ☐ 512 ☐ 1024 ☐ 2048 ☐ 4096 ☐ None†

Transmit packet size:

☐ 64 ☐ 128 ☐ 256 ☐ 512 ☐ 1024 ☐ 2048 ☐ 4096 ☐ None†

Receive packet window size: _____

Transmit packet window size: _____

Closed user group index: _____

Closed user group with outgoing access index: _____

User defined facilities: _____

RPOA indices (1-40 decimal digits): _____

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____ Slot _____ Port _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

Port-Level Protocol Parameters

Source Route Bridge

Enable Source Route Bridging on this port:

☐ Enable ☐ Disable†

Ring number (hex)

(Not available for frame relay): _____

Maximum transmission unit (bytes):

- ☐ 516
☐ 1500
☐ 2052†
☐ 4472 (4 Mbps and 16 Mbps token-ring adapter only)
☐ 8144 (16 Mbps token-ring adapter only)
☐ 11407 (16 Mbps token-ring adapter only)
☐ 17800 (16 Mbps token-ring adapter only)

List of Ring Numbers to Frame Relay DLCI Numbers (frame relay only)

Ring Number (hex) (R):

DLCI number (R):

Spanning Tree Parameters

Spanning tree mode: ☐ Automatic† ☐ Manual

Path cost (0-65535) (for automatic only): _____

Enable forwarding of spanning tree packets (for manual only):

☐ Enable† ☐ Disable

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

Port—Level Protocol Parameters

Transparent Bridge

Enable transparent bridging on this port:

☐ Enable ☐ Disable †

Port priority (hex): _____

Determine port state automatically: ☐ Enable † ☐ Disable

Port state: ☐ Forwarding ☐ Disabled †

Path cost: _____

Maximum transmission unit (bytes): _____

List of Frame Relay DLCI Numbers for Transparent Bridge

DLCI number (R):

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____ Slot _____ Port _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

Port-Level Protocol Parameters

Transparent Bridge Inbound Filters

MAC Address

Status of all defined inbound MAC address filters on this port:

☐ Enable† ☐ Disable

Filter Type: ☐ Deny† ☐ Permit

List of Inbound MAC Address Filters (Source - Destination)

Frame Addresses

Source (R): _____

Destination (R): _____

Frame Address Masks

Source Mask: _____

Destination Mask: _____

Source SAP

Status of all defined inbound source SAP filters on this port:

☐ Enable† ☐ Disable

Filter Type: ☐ Deny† ☐ Permit

Frame type: ☐ Single route broadcast (SRB)
☐ All routes broadcast (ARB)
☐ Both SRB and ARB†

List of Inbound Source SAP Filters

Source SAP value (hex) (R): _____

Ethernet Type

Status of all defined inbound Ethernet Type filters on this port:

☐ Enable† ☐ Disable

Filter Type: ☐ Deny† ☐ Permit

List of Inbound Ethernet Type Filters

Ethernet Type value (hex) (R): _____

Ethernet Type value mask (hex) (R): _____

Sliding Window

Status of all defined inbound sliding window filters on this port:

☐ Enable† ☐ Disable

Filter Type: ☐ Deny† ☐ Permit

List of Inbound Sliding Window Filters

Filter Name (R): _____

Offset Starting Field: ☐ MAC† ☐ SAP

Offset Into Frame: _____

Sliding Window Contents (R): _____

Sliding Window Mask (hex): _____

Inbound Filter Order

Change order filters are applied on this port and override system settings: ☐ Enable ☐ Disable†

Source SAP Filter (1-4): _____

Ethernet Type Filter (1-4): _____

MAC Address Filter (1-4): _____

Sliding Window Filter (1-4): _____

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page ____ of ____

Complete one worksheet for each IBM 6611 — Name _____ Slot ____ Port ____

Note: Defaults are noted using a (†) and required information is noted using an (R).

Port-Level Protocol Parameters

Transparent Bridge Outbound Filters

MAC Address

Status of all defined outbound MAC address filters on this port:

☐ Enable† ☐ Disable

Filter Type: ☐ Deny† ☐ Permit

List of Outbound MAC Address Filters (Source - Destination)

Frame Addresses

Source (R): _____

Destination (R): _____

Frame Address Masks

Source Mask: _____

Destination Mask: _____

Source SAP

Status of all defined outbound source SAP filters on this port:

☐ Enable† ☐ Disable

Filter Type: ☐ Deny† ☐ Permit

Frame type: ☐ Single route broadcast (SRB)
☐ All routes broadcast (ARB)
☐ Both SRB and ARB†

List of Outbound Source SAP Filters

Source SAP value (hex) (R): _____

Ethernet Type

Status of all defined outbound Ethernet Type filters on this port:

☐ Enable† ☐ Disable

Filter Type: ☐ Deny† ☐ Permit

List of Outbound Ethernet Type Filters

Ethernet Type value (hex) (R): _____

Ethernet Type value mask (hex) (R): _____

Sliding Window

Status of all defined outbound sliding window filters on this port:

☐ Enable† ☐ Disable

Filter Type: ☐ Deny† ☐ Permit

List of Outbound Sliding Window Filters

Filter Name (R): _____

Offset Starting Field: ☐ MAC† ☐ SAP

Offset Into Frame: _____

Sliding Window Contents (R): _____

Sliding Window Mask (hex): _____

Outbound Filter Order

Change order filters are applied on this port and override system settings: ☐ Enable ☐ Disable†

Source SAP Filter (1-4): _____

Ethernet Type Filter (1-4): _____

MAC Address Filter (1-4): _____

Sliding Window Filter (1-4): _____

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____ Slot _____ Port _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

Port-Level Protocol Parameters

Source Route Bridge Inbound Filters

MAC Address

Status of all defined inbound MAC address filters on this port:

☐ Enable† ☐ Disable

Filter Type: ☐ Deny† ☐ Permit

Frame Type: ☐ Single route broadcast (SRB)

☐ All routes broadcast (ARB)

☐ Both SRB and ARB†

List of Inbound MAC Address Filters (Source - Destination)

Frame Addresses

Source (R): _____

Destination (R): _____

Frame Address Masks

Source Mask: _____

Destination Mask: _____

Source SAP

Status of all defined inbound source SAP filters on this port:

☐ Enable† ☐ Disable

Filter Type: ☐ Deny† ☐ Permit

Frame type: ☐ Single route broadcast (SRB)

☐ All routes broadcast (ARB)

☐ Both SRB and ARB†

List of Inbound Source SAP Filters

Source SAP value (hex) (R): _____

SNAP Value

Status of all defined inbound SNAP filters on this port:

☐ Enable† ☐ Disable

Filter Type: ☐ Deny† ☐ Permit

List of Inbound Source SNAP Filters

SNAP value (hex) (R): _____

SNAP value mask (hex) (R): _____

Ring Number

Status of all defined inbound ring number filters on this port:

☐ Enable† ☐ Disable

Filter Type: ☐ Deny† ☐ Permit

Frame Type: ☐ Single route broadcast (SRB)

☐ All routes broadcast (ARB)

☐ Both SRB and ARB†

List of Inbound Ring Number Filters

Ring number (hex) (R): _____

Ring Number mask (hex) (R): _____

Sliding Window

Status of all defined inbound sliding window filters on this port:

☐ Enable† ☐ Disable

Filter Type: ☐ Deny† ☐ Permit

Frame Type: ☐ Single route broadcast (SRB)

☐ All routes broadcast (ARB)

☐ Both SRB and ARB†

List of Inbound Sliding Window Filters

Filter Name (R): _____

Offset Starting Field: ☐ MAC† ☐ SAP

Offset Into Frame: _____

Sliding Window Contents (R): _____

Sliding Window Mask (hex): _____

Inbound Filter Order

Change order filters are applied on this port and override system settings: ☐ Enable ☐ Disable†

Hop Count Filter (1-6): _____

Source SAP Filter (1-6): _____

SNAP Value Filter (1-6): _____

Ring Number Filter (1-6): _____

MAC Address Filter (1-6): _____

Sliding Window Filter (1-6): _____

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page ____ of ____

Complete one worksheet for each IBM 6611 — Name _____ Slot ____ Port ____

Note: Defaults are noted using a (†) and required information is noted using an (R).

Port-Level Protocol Parameters

IP

Enable IP routing on this port: ☐ Enable ☐ Disable†

IP address (R): _____

Subnet mask: _____

Destination IP address
(for PPP on a Serial Adapter) (R): _____

Maximum transmission unit (bytes): _____

(Ethernet adapter only)

Ethernet framing for IP:

☐ Both

☐ Ethernet Version 2†

☐ 802.3 SNAP

Filter IP address 2:

Filter subnet mask 2:

IP Port Filters

Status of all defined IP port filters: ☐ Enable† ☐ Disable

List of IP Port Filters (Filter ID)

IP filter ID (1-100) (R):

Filter type: ☐ Singular† ☐ Dual

Permit/deny traffic: ☐ Deny ☐ Permit†

Filter IP address 1 (R):

Filter subnet mask 1:

Define IP Destinations Per DLCI (Frame relay only)

List of DLCI Numbers to IP Destinations (Optional)

Destination address:

DLCI number:

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page ____ of ____

Complete one worksheet for each IBM 6611 — Name _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

Port—Level Protocol Parameters

AppleTalk

Enable AppleTalk routing on this port:

☐ Enable ☐ Disable †

Define Port Characteristics

Port type: ☐ Nonseed router port † ☐ Seed router port

Network number range: _____

Default zone name (ASCII): _____

Starting value for node ID acquisition: _____

Define Additional Zone Names for Network Zone List

Additional zone name (ASCII): _____

Define AppleTalk Filters for the Port

Enable security filters: ☐ Enable ☐ Disable †

Enable network number range filter: ☐ Enable ☐ Disable †

List of Network Number Ranges

Network number range (R): _____

Define DLCI Numbers for Frame Relay Connection

DLCI Number (R): _____

Accept routing information:

☐ About all networks † ☐ ONLY about selected networks

List of Selected Networks

Network number range (R): _____

Filter Traffic to and from Selected Networks

Enable network number range filter: Enable Disable †

List of Network Number Ranges to Filter

Network number range (R): ☐ ☐

Define Allowable Zones for Selected Networks

Allowable zone name (R) (ASCII): _____

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page ____ of ____

Complete one worksheet for each IBM 6611 — Name _____ Slot ____ Port ____

Note: Defaults are noted using a (†) and required information is noted using an (R).

Port-Level Protocol Parameters

IPX

Enable IPX routing on this port: ☐ Enable ☐ Disable†

IPX network number (R): _____

Destination host address
(for PPP on a serial adapter) (R): _____

Encapsulation Method:

(For Token-Ring Network 16/4 Adapter)

☐ Token-Ring 802.5†

☐ Token-Ring SNAP

(For Ethernet Adapter)

☐ Ethernet Version 2

☐ Ethernet SNAP

☐ Ethernet 802.3†

☐ Ethernet 802.2

Software loopback active: ☐ Enable† ☐ Disable

Define IPX Destinations Per DLCI

List of DLCI Numbers to IPX Destinations (Optional)

Destination IPX address:

DLCI number:

Define IPX Port Filters

Status of all defined IPX filters on this port:

☐ Enable† ☐ Disable

Filtering mode: ☐ Deny† ☐ Permit

List of Port Filters

Filter ID (1-10) (R): _____

Filter on packet type: ☐ Enable ☐ Disable†

Pack type value (hex) (R): _____

Transport Control Attributes

Filter on transport control: ☐ Enable ☐ Disable†

Transport control value (hex) (R): _____

Relational compare operator:

☐ Equals†

☐ Less than

☐ Less than or equal

☐ Greater than

☐ Greater than or equal

Destination Attributes

Filter based on destination network: ☐ Enable ☐ Disable†

Destination network value (hex) (R): _____

Filter on destination host: ☐ Enable ☐ Disable†

Destination host value (hex) (R): _____

Filter on destination socket: ☐ Enable ☐ Disable†

Destination socket value (hex) (R): _____

Source Attributes

Filter on source network: ☐ Enable ☐ Disable†

Source network value (hex) (R): _____

Filter on source host: ☐ Enable ☐ Disable†

Source host value (hex) (R): _____

Filter on source socket: ☐ Enable ☐ Disable†

Source socket value (hex) (R): _____

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____ Slot _____ Port _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

Port-Level Protocol Parameters

XNS

Enable XNS routing on this port: ☐ Enable ☐ Disable†

XNS network number (R): _____

Destination host address

(for PPP on a Serial Adapter) (R): _____

Encapsulation Method:

(For Token-Ring Network 16/4 Adapter)

☐ Token-Ring 802.5

☐ Token-Ring SNAP†

(For Ethernet Adapter)

☐ Ethernet Version 2†

☐ Ethernet SNAP

☐ Ethernet 802.3

Number of bytes returned

in an error protocol packet: _____

Error protocol active: ☐ Enable† ☐ Disable

Software loopback active: ☐ Enable† ☐ Disable

Define XNS Destinations Per DLCI

List of DLCI Numbers to XNS Destinations (Optional)

Destination XNS address:

DLCI number:

Define XNS Port Filters

Status of all defined XNS filters on this port:

☐ Enable† ☐ Disable

Filtering mode: ☐ Deny† ☐ Permit

List of Port Filters

Filter ID (1-10) (R): _____

Filter based on checksum: ☐ Enable ☐ Disable†

Checksum value (hex) (R): _____

Filter on packet type: ☐ Enable ☐ Disable†

Pack type value (hex) (R): _____

Transport Control Attributes

Filter on transport control: ☐ Enable ☐ Disable†

Transport control value (hex) (R): _____

Relational compare operator:

☐ Equals

☐ Less than

☐ Less than or equal

☐ Greater than

☐ Greater than or equal

Destination Attributes

Filter based on destination network: ☐ Enable ☐ Disable†

Destination network value (hex) (R): _____

Filter on destination host: ☐ Enable ☐ Disable†

Destination host value (hex) (R): _____

Filter on destination socket: ☐ Enable ☐ Disable†

Destination socket value (hex) (R): _____

Source Attributes

Filter on source network: ☐ Enable ☐ Disable†

Source network value (hex) (R): _____

Filter on source host: ☐ Enable ☐ Disable†

Source host value (hex) (R): _____

Filter on source socket: ☐ Enable ☐ Disable†

Source socket value (hex) (R): _____

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page ____ of ____

Complete one worksheet for each IBM 6611 — Name _____ Slot ____ Port ____

Note: Defaults are noted using a (†) and required information is noted using an (R).

Port-Level Protocol Parameters

DECnet

Enable DECnet on this interface: ☐ Enable ☐ Disable †

Remote DECnet address:

Remote DECnet address

(PPP on a serial adapter) (R): _____

(PPP only)

Remote DECnet node type: ☐ Area
☐ Routing IV †
☐ End node

Remote DECnet node type: ☐ Area †
☐ Routing IV
☐ End node

Circuit cost (1-63): _____

Hello timer (1-8191 seconds): _____

Router priority (0-127): _____

Routing timer (1-65535 seconds): _____

Maximum routers (1-1022): _____

Define Port Filters

Status of all defined DECnet filters on this port: ☐ Enable †
☐ Disable

Define DECnet Destinations Per DLCI

(Frame relay only)

List of DLCI Numbers to DECnet Destinations (Optional)

DLCI number:

List of Packet Filters (Filter ID)

Filter ID (1-100) (R):

Direction in which packet is moving:

☐ Inbound
☐ Outbound
☐ Inbound and Outbound †

IBM 6611 Network Processor Configuration Worksheet

Completed by: _____ Date _____ Page _____ of _____

Complete one worksheet for each IBM 6611 — Name _____ Slot _____ Port _____

Note: Defaults are noted using a (†) and required information is noted using an (R).

Port-Level Protocol Parameters

SNA

Enable SNA frame forwarding on this port:

- ☐ Enable
☐ Disable†

List of SAP Values for Frame Forwarding

SAP Value (hex) (R):

NetBIOS

Forward NetBIOS frames on this port:

- ☐ Enable
☐ Disable†

Forward NetBIOS datagram and datagram broadcast message on this port:

- ☐ Enable†
☐ Disable

Appendix B. Error and Status Codes

There are two types of error or status codes. They are alphanumeric and numeric. The alphanumeric codes (codes that are non-service codes) are listed in this section. The numeric codes are service error codes and are listed in the *6611 Network Processor Installation and Service Guide*.

Code	Message	User Response/Action
0c0	A user-requested dump has been completed successfully.	Progression indicator; no action.
0c2	A user-requested dump has started.	Progression indicator; no action.
0c3	The dump is inhibited.	The dump procedure cannot be performed at this time. Regenerate the failing operational scenario and perform the dump procedure correctly once the operational problem has been re-created.
0c4	The dump was not completed. A partial dump may be present.	Check the dump device for partial dump output. Retrieve the partial dump output. Regenerate the failing operational scenario and perform the dump procedure correctly once the operational problem has been re-created.
0c5	The dump has failed to start. The dump program did not write to the dump device.	Check the dump device for readiness and correct diskette format. Regenerate the failing operational scenario and perform the dump procedure correctly once the operational problem has been re-created.
0c8	The dump is disabled. The system configuration does not include a dump device for the requested dump.	Configure for and specify the dump device. Regenerate the failing operational scenario and perform the dump procedure correctly once the operational problem has been re-created.
0c9	A system initiated dump is in progress. An unexpected system halt occurred and a system dump has started automatically.	Progression indicator; no action.
10c	The system monitor process cannot access the adapter installed in slot 1 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
11c	The system monitor process cannot access the Internet Protocol (IP) function code on the adapter installed in slot 1 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.

Code	Message	User Response/Action
12c	The system monitor process cannot access the XNS** function code on the adapter installed in slot 1 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
13c	The system monitor process cannot access the DECnet** function code on the adapter installed in slot 1 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
14c	The system monitor process cannot access the Internet Packet Exchange (IPX) function code on the adapter installed in slot 1 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
15c	The system monitor process cannot access the AppleTalk function code on the adapter installed in slot 1 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
1c1	Starting IP routing protocols process.	Progression indicator; no action.
1c2	The system monitor process cannot start the IP routing protocols process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time. 6. Possible hardware error.	Progression indicator. IP routing protocols are disabled upon IPL completion. Run box hardware diagnostics.
1c3	Starting configuration error process.	Progression indicator; no action.
1c4	The system monitor process cannot start the configuration error process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. Configuration errors will not be tracked upon IPL completion.
1c5	Starting protocol configuration process.	Progression indicator; no action.

Code	Message	User Response/Action
1c6	The system monitor process cannot start the protocol configuration process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. No protocols will be operational upon IPL completion.
1c7	Starting peer-capable adapter error log process.	Progression indicator; no action.
1c8	The system monitor process cannot start the peer-capable adapter error log process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. Error logging on peer-capable cards will not occur upon IPL completion.
1c9	Starting IP routing protocol configuration process.	Progression indicator; no action.
20c	The system monitor process cannot access the adapter installed in slot 2 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
21c	The system monitor process cannot access the IP function code on the adapter installed in slot 2 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
22c	The system monitor process cannot access the XNS function code on the adapter installed in slot 2 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
23c	The system monitor process cannot access the DECnet function code on the adapter installed in slot 2 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.

Code	Message	User Response/Action
24c	The system monitor process cannot access the IPX function code on the adapter installed in slot 2 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
25c	The system monitor process cannot access the AppleTalk function code on the adapter installed in slot 2 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
2c0	Software is locked.	Progression indicator. IPL is halted. Software must be unlocked before to successful IPL completion. Check configuration and check with your system administrator.
2c1	Checking software lock.	Progression indicator; no action.
2c2	Getting configuration data.	Progression indicator; no action.
2c4	Starting IP protocol process.	Progression indicator; no action.
2c5	Starting XNS protocol process.	Progression indicator; no action.
2c6	Starting DECnet protocol process.	Progression indicator; no action.
2c7	Starting SNMP protocol process.	Progression indicator; no action.
2c8	Starting DLS protocol process.	Progression indicator; no action.
2c9	Starting SNA protocol process.	Progression indicator; no action.
30c	The system monitor process cannot access the adapter installed in slot 3 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
31c	The system monitor process cannot access the IP function code on the adapter installed in slot 3 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
32c	The system monitor process cannot access the XNS function code on the adapter installed in slot 3 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.

Code	Message	User Response/Action
33c	The system monitor process cannot access the DECnet function code on the adapter installed in slot 3 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
34c	The system monitor process cannot access the IPX function code on the adapter installed in slot 3 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
35c	The system monitor process cannot access the AppleTalk function code on the adapter installed in slot 3 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
3c0	Starting the system monitor process.	Progression indicator; no action.
3c1	Starting the process monitor process.	Progression indicator; no action.
3c2	Starting the disk monitor process.	Progression indicator; no action.
3c3	Starting the interface monitor process.	Progression indicator; no action.
3c4	Starting the protocol monitor process.	Progression indicator; no action.
3c7	Starting the IPX protocol process.	Progression indicator; no action.
3c8	Starting the X.25 process.	Progression indicator; no action.
3c9	Starting the smart card routing adapter management process.	Progression indicator; no action.
40c	The system monitor process cannot access the adapter installed in slot 4 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
41c	The system monitor process cannot access the IP function code on the adapter installed in slot 4 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.

Code	Message	User Response/Action
42c	The system monitor process cannot access the XNS function code on the adapter installed in slot 4 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
43c	The system monitor process cannot access the DECnet function code on the adapter installed in slot 4 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
44c	The system monitor process cannot access the IPX function code on the adapter installed in slot 4 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
45c	The system monitor process cannot access the AppleTalk function code on the adapter installed in slot 4 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
4c0	Starting the configuration process.	Progression indicator; no action.
4c1	The system monitor process cannot start the IP routing protocols configuration process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. IP routing protocols will be disabled upon IPL completion.
4c2	Starting IBM Token-Ring Network Remote Bridge Program point-to-point protocol process.	Progression indicator; no action.
4c3	Starting bridge spanning tree main process.	Progression indicator; no action.
4c4	Starting configuration point-to-point protocol process.	Progression indicator; no action.
4c5	Starting point-to-point protocol system monitor process.	Progression indicator; no action.

Code	Message	User Response/Action
4c6	The system monitor process cannot start the point-to-point protocol system monitor process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. IP point-to-point protocol will not operate upon IPL completion.
4c7	Starting transparent bridging spanning tree main process.	Progression indicator; no action.
4c8	Starting AppleTalk protocol process.	Progression indicator; no action.
4c9	Starting APPN Program process.	Progression indicator; no action.
4cc	Starting asynchronous routing communication.	Progression indicator; no action.
50c	The system monitor process cannot access the adapter installed in slot 5 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
51c	The system monitor process cannot access the IP function code on the adapter installed in slot 5 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
52c	The system monitor process cannot access the XNS function code on the adapter installed in slot 5 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
53c	The system monitor process cannot access the DECnet function code on the adapter installed in slot 5 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
54c	The system monitor process cannot access the IPX function code on the adapter installed in slot 5 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.

Code	Message	User Response/Action
55c	The system monitor process cannot access the AppleTalk function code on the adapter installed in slot 5 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
5c5	The system monitor process cannot start the <i>IBM Token-Ring Network Transparent Bridge Program</i> process due to the following representative errors: 1. Process crash. 2. Process hung waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. The Transparent bridge spanning tree function is disabled upon IPL completion.
5c6	The system monitor process cannot start the AppleTalk protocol process due to the following representative errors: 1. Process crash. 2. Process hung waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. AppleTalk protocol is disabled upon IPL completion.
5c7	The system monitor process cannot start the asynchronous routing communication process due to the following representative errors: 1. Process crash. 2. Process hung waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. Asynchronous routing communication is disabled upon IPL completion.
60c	The system monitor process cannot access the adapter installed in slot 6 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
61c	The system monitor process cannot access the IP function code on the adapter installed in slot 6 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
62c	The system monitor process cannot access the XNS function code on the adapter installed in slot 6 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.

Code	Message	User Response/Action
63c	The system monitor process cannot access the DECnet function code on the adapter installed in slot 6 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
64c	The system monitor process cannot access the IPX function code on the adapter installed in slot 6 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
65c	The system monitor process cannot access the AppleTalk function code on the adapter installed in slot 6 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
70c	The system monitor process cannot access the adapter installed in slot 7 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
71c	The system monitor process cannot access the IP function code on the adapter installed in slot 7 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
72c	The system monitor process cannot access the XNS function code on the adapter installed in slot 7 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
73c	The system monitor process cannot access the DECnet function code on the adapter installed in slot 7 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.

Code	Message	User Response/Action
74c	The system monitor process cannot access the IPX function code on the adapter installed in slot 7 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
75c	The system monitor process cannot access the AppleTalk function code on the adapter installed in slot 7 due to a problem with: 1. System code that communicates with the adapter. 2. Adapter microcode. 3. Adapter hardware.	For suspected software problem: check error log to determine software problem. For suspected hardware problem: 1. Perform adapter diagnostics. 2. Check the adapter for correct installation. 3. Check the adapter for defects.
80c	The system monitor process cannot start the configuration process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. IPL does not complete successfully. System Manager functions are still operational.
81c	The system monitor process cannot start the disk monitor process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	The disk monitor function is disabled upon IPL completion. The system monitor is not able to identify disk errors and status.
82c	The system monitor process cannot start the DECnet routing process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. DECnet routing is disabled upon IPL completion.
83c	The system monitor process cannot start the process monitor process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. The process monitor function is disabled upon IPL completion. The system monitor is not able to identify process errors and status for those processes that it monitors.

Code	Message	User Response/Action
84c	The system monitor process cannot start the smart card routing adapter management process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. Routing and bridging functions related to the peer-capable, forwarding adapters is not operational.
85c	The system monitor process cannot start the protocol monitor process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. The protocol monitor function is disabled upon IPL completion. The system monitor is not able to identify protocol errors and status for protocol processes that it monitors.
87c	The system monitor process cannot start the XNS routing process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. XNS routing is disabled upon IPL completion.
88c	The system monitor process cannot start the IPX routing process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. IPX routing is disabled upon IPL completion.
89c	The system monitor process cannot start the X.25 process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. The X.25 function is disabled upon IPL completion.
90c	The system monitor process cannot start the SNMP process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. SNMP network management is disabled upon IPL completion.

Code	Message	User Response/Action
91c	The system monitor process cannot start the SNMP trap subagent process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. The SNMP trap function is disabled upon IPL completion.
92c	The <i>system monitor</i> process cannot start the <i>SNMP subagent</i> process that handles bridging, DECnet, XNS, IPX, frame relay, system, Ethernet, Token Ring, and NetView/6000 functions due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. The IBM 6611 SNMP subagent that handles the functions listed is disabled upon IPL completion.
93c	The system monitor process cannot start the SNMP subagent process that handles DS1 (T1) service and Cylink functions due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. The IBM 6611 SNMP subagent that handles the functions listed is disabled upon IPL completion.
94c	The system monitor process cannot start the SNMP subagent process that handles IP, ICMP, interface (if), interface extensions (ifExtensions), address translation (at), and peer-capable, forwarding adapter functions due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. The IBM 6611 SNMP subagent that handles the functions listed is disabled upon IPL completion.
95c	The system monitor process cannot start the SNMP PPP subagent process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. The IBM 6611 SNMP PPP subagent is disabled upon IPL completion.

Code	Message	User Response/Action
96c	The system monitor process cannot start the configuration process subagent process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. The IBM 6611 configuration process subagent is disabled upon IPL completion.
97c	The system monitor process cannot start the IBM Token-Ring Network Remote Bridge Program process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. The IBM Token-Ring Remote Bridge Program function is disabled upon IPL completion.
98c	The system monitor process cannot start the bridge spanning tree main process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. The bridge spanning tree function is disabled upon IPL completion.
99c	The system monitor process cannot start the DLS initialization process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. The DLS function is disabled upon IPL completion.
c20	The system debug program is activated due to an unexpected system halt that has occurred.	Progression indicator; a flashing 888 is displayed and a system dump is performed after c20 is displayed.
c31	There is no terminal attached to serial port S1 or S2 to provide a console for stand-alone diagnostics.	Select a console terminal for diagnostics via the following procedure: 1. Attach a terminal to either serial port (Serial 1 or S1 preferred). 2. Enter a 1. Diagnostic instructions and subsequent menus will be displayed. If you do not require a diagnostic console, set the key mode switch to the Normal position and then back to the Service position. This will cause the diagnostic programs to load and perform the diagnostics automatically.

Code	Message	User Response/Action
c33	The system is attempting to access an ASCII terminal or PC with ASCII terminal emulator program attached to the S1 serial port.	Verify correct terminal attachment to the Serial port. 1. If no terminal is attached to serial 1 or S1 port, attach an ASCII terminal or PC with an ASCII terminal emulator program to Serial 1 or S1 port and turn on the terminal. Operation resumes normally. 2. If a terminal is attached to Serial 1 or S1 port, perform a power-on-reset for that terminal. Operation resumes normally.
c34	The system is attempting to access an ASCII terminal or PC with ASCII terminal emulator program or modem attached to the S2 serial port.	Verify correct terminal or modem attachment to the Serial port. 1. If no terminal or modem is attached to serial 2 or S2 port, attach an ASCII terminal or PC with an ASCII terminal emulator program to Serial 2 or S2 port and turn on the terminal. Operation resumes normally. 2. If a terminal or modem is attached to Serial 2 or S2 port, perform a power-on-reset for that device. Operation resumes normally.
c40	The system monitor process cannot start the PPP configuration process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. The PPP configuration function is disabled upon IPL completion.
c41	The system monitor process cannot start the interface monitor process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. The interface monitor function is disabled upon IPL completion. The system monitor is not able to identify interface errors and status for interfaces that it monitors.
c42	The system monitor process cannot start the SNMP DLS subagent process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. The SNMP DLS subagent function is disabled upon IPL completion.
c43	The system monitor process cannot start the peer-capable, forwarding adapter log process due to the following representative errors: 1. Process crash. 2. Process halted waiting for event trigger. 3. Process start threshold exceeded. 4. Process using too much memory. 5. Process using too much CPU time.	Progression indicator. The peer-capable, forwarding adapter log function is disabled upon IPL completion.
c50	Shutdown has started.	Progression indicator; no action.

Code	Message	User Response/Action
c51	In shutdown procedure, all login is disabled.	Progression indicator; no action.
c52	In shutdown procedure, process accounting has stopped.	Progression indicator; no action.
c53	In shutdown procedure, error logging has stopped.	Progression indicator; no action.
c54	In shutdown procedure, all remote file systems are unmounted.	Progression indicator; no action.
c55	In shutdown procedure, Network File System (NFS) clean is performed.	Progression indicator; no action.
c56	In shutdown procedure, TCP clean is performed.	Progression indicator; no action.
c57	In shutdown procedure, all files systems are unmounted.	Progression indicator; no action.
c58	In shutdown procedure, all SRC subsystems have stopped.	Progression indicator; no action.
c59	In shutdown procedure, respawning of processes has stopped.	Progression indicator; no action.
c60	In shutdown procedure, the system is coming to a complete halt.	Progression indicator; no action.
c61	In shutdown procedure, the system is going into maintenance mode.	Progression indicator; no action.
c67	Configuration diskette not present.	Progression indicator; the configuration process temporarily waits for problem resolution. Insert the configuration diskette in the diskette drive. For initial configuration, IPL operation continues if the diskette is inserted within 1 minute; after 1 minute, reinitiate the IPL operation with the configuration diskette in the diskette drive. For subsequent configurations, normal operation continues with the previous configuration active until the new configuration diskette has been installed and the update sequence invoked from the System Manager.
c68	Configuration diskette not readable.	Progression indicator; the configuration process temporarily waits for problem resolution. Format the configuration diskette using DOS or insert a formatted DOS configuration diskette. For initial configuration, IPL operation continues if the diskette is readable and inserted within 1 minute; after 1 minute, reinitiate the IPL operation with a readable configuration diskette inserted. For subsequent configurations, normal operation continues with the previous configuration active until the new configuration diskette has been installed and the update sequence invoked from the System Manager.

Code	Message	User Response/Action
c69	Configuration file not present on the diskette in the diskette drive.	Progression indicator; the configuration process temporarily waits for problem resolution. Check the inserted diskette for configuration file. Insert the diskette with correct configuration file present. For initial configuration, IPL operation continues if the diskette is made readable and inserted within 1 minute; after 1 minute, reinitiate the IPL operation with the configuration file present on the diskette. For subsequent configurations, normal operation continues with the previous configuration active until the new configuration file is present on the diskette and the update sequence has been invoked from the System Manager.
c70	Incorrect configuration file format (not binary).	Progression indicator; the configuration process temporarily waits for problem resolution. Regenerate the configuration file in binary format and insert the diskette, or resend the binary file. For initial configuration, IPL operation continues if the correct file format is generated and the diskette is inserted within 1 minute; after 1 minute, reinitiate the IPL operation with the configuration diskette inserted. For subsequent configurations, normal operation continues with the previous configuration active until the new configuration file is present on the diskette or sent via the network. System Manager is required to invoke the update sequence if it is from the diskette.
c71	Configuration diskette not writeable.	Progression indicator; the configuration process temporarily waits for problem resolution. Remove write protection on the diskette. For initial configuration, IPL operation continues if the diskette is writeable and inserted within 1 minute; after 1 minute, reinitiate the IPL operation with the writable configuration diskette inserted. For subsequent configurations, normal operation continues with the previous configuration active until the diskette is writable and the update sequence invoked from the System Manager.
c72	Configuration errors detected after the configuration file is received. Representative errors include: 1. Incorrect configuration data in file. 2. Configuration data and hardware mismatch. 3. Function validity. 4. Function interdependency error.	Check the error log for error details. Resolve the configuration error. For initial configuration, reinitiate the IPL procedure with the corrected configuration. For subsequent configurations, normal operation continues with the previous configuration active until the new configuration is available (configuration errors are resolved).

Code	Message	User Response/Action
c73	Wrong configuration program version number. The version of the configuration program must match the version of the Multiprotocol Network Program.	Acquire the correct configuration program version and ensure that it matches the Multiprotocol Network Program version. Reconfigure it if necessary. Apply matching configuration version to IBM 6611 with matching Multiprotocol Network Program version. Normal operation continues with the previous configuration active until the configuration and code versions are matched.
c74	Wrong 6611 model number. The model number in the configuration file does not match the model number of the IBM 6611.	Reconfigure the model number response. For initial configuration, reinitiate the IPL operation after the model number configured matches the machine model to which it is being applied. For subsequent configurations, normal operation continues with the previous configuration active until the configuration model and machine model are matched (new configuration file is available).
c80	6611 is activating all configured network adapters.	Progression indicator; no action.
c81	Configuration data has changed that requires the machine to be reinitialized (IPL). The IPL is in progress.	Progression indicator; no action.
c89	The configuration process is complete. The adapters are initialized.	Progression indicator; no action.
c99	Diagnostics are complete.	Progression indicator; no action. This code is only used when there is no terminal attached to port 1.

Appendix C. License Program Specification

This appendix contains license information about the IBM Multiprotocol Network Program Version 1 Release 1.1 and Version 1 Release 1.2. The product identifier for this product is 5648-016.

Description

The IBM Multiprotocol Network Program Version 1 provides bridging and routing software for the IBM 6611 Network Processor. All models are shipped with the Multiprotocol Network Program installed.

The basic functions of the Multiprotocol Network Program include:

- The ability to route a variety of protocols such as IP, IPX, XNS, AppleTalk, APPN, and DECnet
- The ability to transport Systems Network Architecture (SNA) and Network Basic Input/Output Systems (NetBIOS) traffic using data link switching in a bridged or routed environment
- A Simple Network Management Protocol (SNMP) network management agent.

Included with the IBM Multiprotocol Network Program are two other programs, which complete the software product:

- The IBM Multiprotocol Network Program System Manager is an interactive user interface designed to perform system management and operation tasks. It displays a hierarchy of menus that lead to interactive dialogs. The System Manager is installed on the IBM 6611 Network Processor.
- The IBM Multiprotocol Network Program Configuration Program is a graphical user interface designed to configure the IBM 6611 Network Processor. The Configuration Program diskettes are shipped with the IBM 6611. Store the Configuration Program diskettes in the binder for this book. The Configuration Program is operated on a RISC System/6000 or PS/2 workstation.

Specified Operating Environment

Machine Requirements

The IBM Multiprotocol Network Program is designed to operate on the IBM 6611 Network Processor. The minimal machine configuration consists of an IBM 6611 Network Processor and the communication adapters required to implement the user's configuration.

To run diagnostics after installing or servicing the IBM 6611, it is required that the user make an ASCII terminal such as the IBM 3161 or an equivalent available to IBM service personnel. In normal operating mode, the IBM 6611 and the Multiprotocol Network Program will not use the ASCII terminal.

IBM will provide optional remote service capability for IBM 6611 users. Customers who want to establish this service must provide a modem such as the IBM 5853, or an equivalent, and a communications line.

Programming Requirements

Initial configuration of the Multiprotocol Network Program and subsequent configuration changes can be performed using the IBM Multiprotocol Network Program Configuration Program or the IBM Multiprotocol Network Program System Manager. The Configuration Program will operate in either of the following user-supplied hardware and software operating environments:

- An IBM PS/2 or compatible workstation using:
 - An Intel 80386 or higher central processing unit
 - IBM DOS 3.3 or Microsoft DOS 3.3 or later
 - Microsoft Windows 3.0 or later
 - 8 MB of memory
 - 3.5-inch diskette drive
 - 10 MB of available disk drive space
 - VGA display
 - Mouse.
- A RISC System/6000 workstation using:
 - AIX Version 3.1.5 or later versions
 - AIX windows
 - 16 MB of memory
 - 3.5-inch diskette drive
 - 10 MB of available disk drive space
 - Graphics display
 - Mouse.

If the user wants to install a communication link between the Configuration Program on a RISC System/6000 workstation and the IBM 6611, the TCP/IP function in AIX 3.1.5 must be installed.

If the user wants to use the network management capability, the SNMP agent must be configured in the Multiprotocol Network Program. In addition, the user must install an SNMP network manager such as the IBM AIX NetView/6000 (5765-077).

If the user wants to install remote source route bridging, the function must be configured in the Configuration Program. Remote source route bridging can be implemented by using the IBM 6611 for each bridge half, or by using the IBM 6611 for one half and an IBM PS/2 workstation for the other bridge half. If the latter option is selected, the PS/2 workstation must have the IBM Token-Ring Network Bridge Program Version 2.2 (53F7724) installed. If the user wants to implement network management of the IBM Token-Ring Network, the IBM LAN Network Manager Version 1.0 (74F5537) must be installed on the PS/2 workstation.

Note: The user cannot create a backup copy of the Multiprotocol Network Program.

Licensed Program Materials Availability

Yes. This licensed program is available with some licensed program materials designated as "RESTRICTED MATERIALS OF IBM." The remaining licensed program materials are available and are not designated as "RESTRICTED MATERIALS OF IBM."

Supplemental Terms

Testing Period

None

Installation/Location License

Not applicable. A separate license is required for each machine on which the license program will be used.

Selling to a Third Party: When the IBM 6611 is sold to a third party, the original owner must lock the Multiprotocol Network Program using either the Configuration Program or a fast-path command primitive. The software is locked by the original owner and unlocked by the customer to whom it was sold.

Usage License

Not applicable.

Type/Duration of Program Services

Central Service, including the IBM Support Center, will be available until discontinued by IBM with a minimum of six months written notice.

Warranty

IBM warrants that:

1. IBM has the right to license this program.
2. The IBM program conforms to its specifications.

The warranty period for this program expires when its program services are no longer available. During the warranty period, IBM will provide warranty service, without charge, through Program Services. Program Services are available for a warranty program for at least one year following the program's general availability.

Additional Information

Any other documentation with respect to this licensed program, including any documentation referenced herein, is provided for reference purposes only and does not extend or modify these specifications.

List of Abbreviations and Acronyms

AARP	AppleTalk Address Resolution Protocol	IPX	Internetwork Packet Exchange
AIX	Advanced Interactive Executive	ISO	International Organization of Standardization
APAR	authorized program analysis report	KB	kilobyte
APPN	Advanced Peer-to-Peer Networking	LAN	local area network
ARP	Address Resolution Protocol	LCN	logical channel number
AS	Autonomous System	LLC	logical link control
ASN	Autonomous System Number	LMI	Local Management Interface
ASE	autonomous system externals	MAC	medium access control
ASCII	American National Standard Code for Information Interchange	MB	megabyte
AT	Attention Command Set	Mbps	megabits per second
ATP	AppleTalk Transaction Protocol	MIB	management information base
BGP	Border Gateway Protocol	MILNET	military network
BIOS	basic input/output	MTU	maximum transmission unit
bps	bits per second	NBP	Name Binding Protocol
CCITT	Consultative Committee on International Telegraph and Telephone	NetBIOS	Network Basic Input/Output System
CE	Customer Engineer	NFS	network file system
CRS	configuration report server	NIC	Network Information Center
CSMD/CD	Carrier Sense Multiple Access with Collision Detection	NRZ	non-return-to-zero
CUG	closed user group	NRZI	non-return-to-zero inverted
DCE	data-circuit terminating equipment	NUA	network user address
DLCI	data link connection identifier	NUI	network user identification
DLS	data link switching	OA	Outgoing Access
DOS	Disk Operating System	OSI	Open Systems Interconnection
DSE	data switching equipment	OSPF	Open Shortest Path First
DSU/CSU	data service unit/channel service unit	OSPFase	Open Shortest Path First autonomous system external links
DTE	data terminal equipment	PC	personal computer
EGP	Exterior Gateway Protocol	PS/2	Personal System/2
EIA	Electronics Industries Association	PPP	Point-to-Point Protocol
FRU	Field Replaceable Unit	PTF	program temporary fix
FTP	File Transfer Protocol	PU	physical unit
HDLC	high-level data link control	PVC	permanent virtual circuit
ICMP	Internet Control Message Protocol	REXEC	Remote Executing Protocol
ID	Identification	RFC	Request For Comments
IEEE	Institute of Electrical and Electronics Engineers	RTMP	Routing Table Maintenance Protocol
IML	initial machine load	RIP	Routing Information Protocol
IP	Internet Protocol	RISC	reduced instruction set computer
IPL	initial program load	ROM	read-only memory
		RPOA	Recognized Private Operating Agency

RR	receiver ready	SVC	switched virtual circuit
RSH	Remote Shell Protocol	TCP	Transmission Control Protocol
SAP	service access point	TCP/IP	Transmission Control Protocol/Internet Protocol
SAP	Service Advertising Protocol	TRB	transparent bridging
SCSI	small computer systems interface	UA	unnumbered acknowledgement
SDLC	synchronous data link control	UDP	User Datagram Protocol
SNA	System Network Architecture	VGA	video graphics adapter
SNAP	Sub-Network Access Protocol	VPD	vital product data
SNMP	Simple Network Management Protocol	XNS	Xerox Network Systems
SRB	source route bridging	ZIP	Zone Information Protocol

Glossary

This glossary includes terms and definitions from:

- The *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Definitions are identified by the symbol (A).
- The *Information Technology Vocabulary*, developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC/JTC1/SC1). Definitions of published parts of this vocabulary are identified by symbol (I); definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T), indicating that final agreement has not been reached among the participating National Bodies of SC1.
- The Network Working Group Request for Comments: 1208.

For a more inclusive list of computer terms and definitions, refer to the *IBM Dictionary of Computing* (SC20-1699).

The following cross references are used in this glossary:

Contrast with: This refers to a term that has an opposed or substantively different meaning.

Synonym for: This indicates that the term has the same meaning as a preferred term, which was defined in its proper place in the glossary.

Synonymous with: This is a backward reference from a defined term to all other terms that have the same meaning.

See: This refers the reader to multiple-word terms that have the same last word.

See also: This refers the reader to related terms that have a related, but not synonymous, meaning.

Deprecated term for: This indicates that the term should not be used. It refers to a preferred term, which is defined in its proper place in the glossary.

A

AARP. AppleTalk Address Resolution Protocol.

abstract syntax notation 1 (ASN.1). The Open Systems Interconnection (OSI) terminology describing abstract syntax. See also *basic encoding rules (BER)*.

ACCESS. In network management, the clause in a Management Information Base (MIB) module that defines the minimum level of support that a managed node provides for an object.

access method. A software component in a processor for controlling the flow of information through a network.

acknowledgment. (1) The transmission, by a receiver, of acknowledge characters as an affirmative response to a sender. (T) (2) An indication that an item sent was received.

active. (1) Operational. (2) Pertaining to a node or device that is connected or is available for connection to another node or device. (3) Able to communicate on the network. A token-ring adapter is active if it is able to transmit and receive on the network.

adapter. A part that electrically or physically connects a device to a computer or to another device.

adapter address. The hexadecimal digits that identify an adapter.

address. The unique code assigned to each device or workstation connected to a network.

addressing. The way in which a station selects the stations to which it is to send data.

address mask. A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. See also *subnet mask*.

address resolution. A method for mapping network layer addresses onto media-specific addresses. See also *Address Resolution Protocol (ARP)*.

Address Resolution Protocol (ARP). A protocol that dynamically maps between Internet addresses, baseband adapter addresses, X.25 addresses, and token-ring adapter addresses on a local area network.

adjacent nodes. Two nodes connected together by at least one path that connects no other node. (T)

Advanced Peer-to-Peer Networking (APPN). An extension to SNA featuring (a) greater distributed network control that avoids critical hierarchical dependencies, thereby isolating the effects of single points of failure; (b) dynamic exchange of network topology information to foster ease of connection, reconfiguration, and adaptive route selection; (c) dynamic definition of network resources; and (d) automated resource registration and directory lookup.

APPN extends the LU 6.2 peer orientation for end-user services to network control and supports multiple LU types, including LU 2, LU 3, and LU 6.2.

Advanced Peer-to-Peer Networking (APPN) end node. A node that provides full SNA end-user services and supports sessions between its local control point (CP) and the CP in an adjacent network node. It uses these sessions to dynamically register its resources with the adjacent CP (its network node server), to send and receive directory search requests, and to obtain management services. An APPN end node can also attach to a subarea network as a peripheral node or to other end nodes.

Advanced Peer-to-Peer Networking (APPN) network. An SNA network that consists of at least one APPN node. An APPN network typically consists of APPN network nodes, APPN end nodes, and, optionally, LEN end nodes.

Advanced Peer-to-Peer Networking (APPN) network node. A node that offers full SNA end-user services and that can provide the following to its local LUs and client end nodes:

- Distributed directory services
- Intermediate routing services within an APPN network
- Network services.

The APPN network node also cooperates with other network nodes to maintain a network topology database, which is used to select optimal routes for LU-LU sessions based on requested classes of service. An APPN network node can also attach to a subarea network as a peripheral node or to other end nodes.

Advanced Peer-to-Peer Networking (APPN) node. An APPN network node or an APPN end node.

advertise. To pass routing reachability information along from one router to another.

agent. In the client-server model, the part of the system that performs information preparation and exchange on behalf of a client or server application. See also *client-server model* and *network management station (NMS)*.

AIX. Advanced interactive executive. See *AIX operating system*.

AIX operating system. IBM's implementation of the UNIX operating system. The RISC System/6000 system, among others, runs on the AIX operating system. See *UNIX operating system*.

AIX NetView/6000. A subset of NetView function that runs on AIX and the RISC System/6000.

all-stations address. Synonym for *broadcast address*.

alternate route. A secondary or backup route that is used if normal routing is not possible.

American National Standards Institute (ANSI). An organization consisting of producers, consumers, and general interest groups, that establishes the procedures by which accredited organizations create and maintain voluntary industry standards in the United States. (A)

analog. (1) Pertaining to data consisting of continuously variable physical quantities. (A)
(2) Contrast with *digital*.

ANSI. American National Standards Institute.

AppleTalk. The routing protocol used to interconnect Apple computers or workstations. AppleTalk groups nodes (hosts) into physical networks corresponding to local area network (LAN) segments or bridged LANs and it allows the logical grouping of hosts (regardless of network boundaries) into AppleTalk zones. The IBM 6611 supports AppleTalk Phase 2 which allows the protocol to handle more complex networks and internets.

AppleTalk Address Resolution Protocol (AARP).
(1) An AppleTalk protocol that provides a translation of AppleTalk node addresses into data link (hardware) addresses. (2) An AppleTalk protocol that reconciles addressing discrepancies in networks that support more than one set of protocols.

AppleTalk Transaction Protocol (ATP). An AppleTalk protocol that provides basic client-server request and response functionality for hosts accessing the Zone Information Protocol (ZIP) for zone information.

application. A network object management process that interacts with the user and is responsible for initiating activity in the system. It does not directly manage any object and can be accessed only by the end user. An application may communicate with object managers, other applications, or user interfaces.

APPN. Advanced Peer-to-Peer Networking.

APPN network. See *Advanced Peer-to-Peer Networking (APPN) network*.

APPN network node. See *Advanced Peer-to-Peer Networking (APPN) network node*.

APPN node. See *Advanced Peer-to-Peer Networking (APPN) node*.

area. As defined by the Internet Protocol (IP), Open Shortest Path First (OSPF), a subset of a network or gateway grouped together by definition of the network administrator. Each area is self-contained; knowledge of an area's topology remains hidden from other areas.

area router. A router used to transmit data within an area. Area routers pass data to backbone routers for inter-area routing.

ARP. Address Resolution Protocol.

ASCII (American Standard Code for Information Interchange). The standard code, using a coded character set consisting of 7-bit coded characters (8-bits including parity check), that is used for information interchange among data processing systems, data communication systems, and associated equipment. The ASCII set consists of control characters and graphics characters. (A)

Note: IBM has defined an extension to ASCII code (characters 128–255).

ASN.1. Abstract syntax notation 1.

ASYNCR. Asynchronous.

asynchronous (ASYNCR). Pertaining to two or more processes that do not depend upon the occurrence of specific events such as common timing signals. (T)

ATP. AppleTalk Transaction Protocol.

auto-call. Synonym for *automatic calling*.

automatic calling. A feature that permits a station to initiate a connection with another station over a switched line without operator action. Synonymous with *auto-call*.

autonomous system. A group of networks and routers under one administrative authority. They cooperate closely to propagate network reachability (and routing) information among themselves using an interior gateway protocol of their choice.

autonomous system number. A number assigned under administrative authority that identifies an autonomous system.

B

backbone. (1) In a local area network multiple-bridge ring configuration, a high-speed link to which the rings are connected by means of bridges or routers. A backbone may be configured as a bus or as a ring. (2) In a wide area network, a high-speed link to which nodes or data switching exchanges (DSEs) are connected.

Basic Input/Output System. See *BIOS*.

baud. (1) A unit of signaling speed equal to the number of discrete conditions or signal events per second; for example, one baud equals one-half dot cycle per second in Morse code, one bit per second in a train of binary signals, and one 3-bit value per second in a train of signals each of which can assume one of

eight different states. (A) (2) In asynchronous transmission, the unit of modulation rate corresponding to one unit interval per second; that is, if the duration of the unit interval is 20 milliseconds, the modulation rate is 50 baud. (A)

best-effort delivery. The unreliable connectionless delivery of datagrams in a network. Information about whether the packet was delivered is not provided to the sender.

BGP. Border Gateway Protocol.

BGP configured neighbor. A specific router (as defined by its BGP neighbor IP address) in a BGP group with which the IBM 6611 Network Processor will exchange routing information.

BGP group. Configured and unconfigured neighbors in the same autonomous system and of the same BGP group type (external, test, internal, or IGP).

BIND. In SNA, a request to activate a session between two logical units (LUs). See also *session activation request*.

BIOS (Basic Input/Output System). In an IBM personal computer, microcode that controls basic hardware operations such as interactions with diskette drives, fixed disk drives, and the keyboard. See *NetBIOS*.

bit clocking. In an EIA 232 interface, the field that indicates which piece of equipment, either the modem or the computer, that provides the clock signal for synchronized data transactions.

block. A string of elements recorded or transmitted as a unit. The elements may be characters, words, or physical records. (T)

Border Gateway Protocol (BGP). An Internet Protocol (IP) routing protocol used between domains and autonomous systems. Contrast with *Exterior Gateway Protocol (EGP)*.

border router. A router, positioned at the edge of an autonomous system, that communicates with a router that is positioned at the edge of a different autonomous system. Synonymous with *boundary router*.

boundary router. Synonym for *border router*.

bps. Bits per second.

bridge. (1) An electronic device that connects multiple networks and enables them to appear as a single segment to all nodes connected to the network. Bridges can selectively repeat data between network segments for X.25 packet switched links, fiber, or satellite communications channels. Contrast with *gateway* and *router*. (2) An attaching device that connects two LAN segments to allow the transfer of information from one LAN segment to the other. The

segments must have the same logical link control (LLC) procedure, but may use different medium access control (MAC) procedures. A bridge may connect the LAN segments directly by network adapters and software in a single device, or may connect network adapters in two separate devices through software and use of a telecommunications link between the two adapters. (3) A device, usually operating at the physical network level, that: (a) connects two or more physical networks and forwards packets between them and (b) stores and forwards complete packets based on physical addresses. (4) In Open Systems Interconnection (OSI), a data link layer intermediate system.

bridge identifier. Used in spanning tree protocol, an 8-byte field composed of the MAC address of the port with the lowest port identifier and a user-defined value.

bridge number. The bridge identifier that the user specifies in the bridge program configuration file. The bridge number distinguishes among parallel bridges.

bridging. The forwarding of a frame from one local area network (LAN) segment to another. The destination is specified by the medium access control (MAC) sublayer address encoded in the destination address field of the frame header.

broadcast. (1) Simultaneous transmission of the same data to more than one destination. (2) A packet delivery system where a copy of a given packet is given to all hosts attached to the network. Broadcast may be implemented in hardware (Ethernet, for example) or software. Contrast with *multicast*.

broadcast address. In SDLC, a station address (eight 1's) reserved as an address common to all stations on a link. Synonymous with *all-stations address*.

bus. (1) A facility for transferring data between several devices located between two end points, only one device being able to transmit at a given moment. (T) (2) A computer configuration in which processors are interconnected in series.

C

cache. (1) A special-purpose buffer storage, smaller and faster than main storage, used to hold a copy of instructions and data obtained from main storage and likely to be needed next by the processor. (T) (2) To place, hide, or store in a cache. (3) An optional part of the directory database in network nodes where frequently used directory information may be stored to speed directory searches.

call-accepted packet. A call supervision packet that a called data terminal equipment (DTE) transmits to indicate to the data circuit-terminating equipment (DCE) that it accepts the incoming call.

call connected packet. A call supervision packet that a data circuit-terminating equipment (DCE) transmits to indicate to a calling data terminal equipment (DTE) that the connection for the call has been completely established.

calling. (1) The process of transmitting selection signals in order to establish a connection between data stations. (A) (I) (2) In X.25 communications, pertaining to the location or user that makes a call.

call request packet. (1) A call supervision packet that a data terminal equipment (DTE) transmits to ask that a connection for a call be established throughout the network. (2) In X.25 communications, a call supervision packet transmitted by a DTE to ask for a call establishment through the network.

carrier. (1) On broadband networks, a continuous frequency signal that can be modulated with an information-carrying signal. (2) An electric or electromagnetic wave or pulse train that may be varied by a signal bearing information to be transmitted over a communication system. (T)

CCITT. The International Telephone and Telegraph Consultative Committee.

CDSTL. Connect data set to line.

central processing unit (CPU). (1) Synonym for processing unit. (T) (2) The part of a computer that includes the circuits that control the interpretation and execution of instructions.

Note: A CPU is the circuitry and storage that executes instructions. Traditionally, the complete processing unit was often regarded as the CPU, whereas today the CPU is often a microchip. In either case, the centrality of a processor or processing unit depends on the configuration of the system or network in which it is used.

change management. The process of planning (for example, scheduling) and controlling (for example, distributing, installing and tracking) changes in an SNA network.

channel. (1) A functional unit, controlled by a processor, that handles the transfer of data between processor storage and local peripheral equipment. See *input/output channel*. (2) A path along which signals can be sent, for example, data channel, output channel. (A)

channel service unit (CSU). A unit that provides the interface to a digital network. The CSU provides line conditioning (or equalization) functions, which keep the signal's performance consistent across the channel bandwidth; signal reshaping, which constitutes the binary pulse stream; and loop-back testing, which includes the transmission of test signals between the

CSU and the network carrier's office channel unit. See *data service unit (DSU)*.

checksum. (1) The sum of a group of data associated with that group and used for checking purposes. (T) (2) In error detection, a function of all bits in a block. If the written and calculated sums do not agree, an error is indicated. (3) On a diskette, data written in a sector for error detection purposes; a calculated checksum that does not match the checksum of data written in the sector indicates a bad sector. The data are either numeric or other character strings regarded as numeric for the purpose of calculating the checksum.

circuit switching. (1) A process that, on demand, connects two or more data terminal equipment (DTEs) and permits the exclusive use of a data circuit between them until the connection is released. (I) (A) (2) Synonymous with *line switching*.

clear indication packet. A call supervision packet that a data circuit-terminating equipment (DCE) transmits to inform a data terminal equipment (DTE) that a call has been cleared.

clear request packet. A call supervision packet transmitted by a data terminal equipment (DTE) to ask that a call be cleared.

client. (1) A user. (2) A functional unit that receives shared services from a server. (T)

client-server model. A common way to describe network services and the user processes (programs) of those services.

clocking. (1) In binary synchronous communication, the use of clock pulses to control synchronization of data and control characters. (2) A method of controlling the number of data bits sent on a telecommunication line at a given time.

closed user group (CUG). In data communication, a group of users who can communicate with other users in the group, but not with users outside the group.

Note: A data terminal equipment (DTE) may belong to more than one closed user group.

closed user group with outgoing access. (1) A closed user group that has a user-assigned facility which enables that user to communicate with others of a data network transmission service where appropriate, with users having a data terminal equipment connected to any other switched network to which interworking facilities are available, or both. (T) (A) (2) In data communication, a closed user group in which one or more users can communicate with users outside the closed group, under certain conditions.

community. An administrative relationship between Simple Network Management Protocol (SNMP) entities.

community name. An opaque string of octets identifying a community.

component. (1) Any part of a network other than an attaching device. (2) Hardware or software that is part of a functional unit.

configuration. (1) The manner in which hardware and software of an information processing system are organized and interconnected. (T) (2) The devices and programs that make up a system, subsystem, or network. (3) The task of defining the hardware and software characteristics of a system or subsystem. See *system configuration*.

configuration file. A file that specifies the characteristics of a system device or network.

configuration management. The control of information necessary to identify both physical and logical information system resources and their relationship to one another.

configuration parameter. A variable in a configuration definition, the value of which characterizes the relationship of a product to other products in the same network.

congestion. See *network congestion*.

connect data set to line (CDSTL). In SNA, an option that determines how the data terminal ready (DTR) signal to the modem operates. It is used if a DTR indicates an unconditional command from the data terminal equipment (DTE) to the attached data circuit-terminating equipment (DCE) to connect to or remove itself from the network.

connection. (1) In data communication, an association established between functional units for conveying information. (I) (A) (2) In Open Systems Interconnection architecture, an association established by a given layer between two or more entities of the next higher layer for the purpose of data transfer. (T) (3) In SNA, the network path that links two logical units (LUs) in different nodes to enable them to establish communications. (4) In X.25 communication, a virtual circuit between two data terminal equipments (DTEs). A switched virtual circuit (SVC) connection lasts for the duration of a call; a permanent virtual circuit (PVC) is a permanent connection between the DTEs. (5) In TCP/IP, the path between two protocol applications that provides reliable data stream delivery service. In Internet, a connection extends from a TCP application on one system to a TCP application on another system. (6) The path between two protocol functions, usually located in different machines, that provides reliable data delivery service.

connectivity. (1) The capability of a system or device to be attached to other systems or devices without modification. (T) (2) The capability to attach a variety of functional units without modifying them.

control point (CP). (1) A component of a node that manages resources of that node and optionally provides services to other nodes in the network. (2) A component of a type 2.1 node that manages the resources of that node. If the type 2.1 node is an APPN node, the CP is capable of engaging in CP-CP sessions with other APPN nodes. If the type 2.1 node is a network node, the CP also provides services to adjacent end nodes in the type 2.1 network.

CP. Control point.

CSU. Channel service unit.

CUG. Closed user group.

D

daemon. In the AIX operating system, a program that runs unattended to perform a standard service. Some daemons are triggered automatically to perform their task; others operate periodically. Synonymous with *demon*.

data circuit. (1) A pair of associated transmit and receive channels that provide a means of two-way data communication. (l) (2) See also *physical circuit* and *virtual circuit*. (3) In SNA, synonym for *link connection*.

Notes:

1. Between data switching exchanges, the data circuit may include data circuit-terminating equipment (DCE), depending on the type of interface used at the data switching exchange.
2. Between a data station and a data switching exchange or data concentrator, the data circuit includes the data circuit-terminating equipment at the data station end, and may include equipment similar to a DCE at the data switching exchange or data concentrator location.

data circuit-terminating equipment (DCE). In a data station, the equipment that provides the signal conversion and coding between the data terminal equipment (DTE) and the line. (l)

Notes:

1. The DCE may be separate equipment or an integral part of the DTE or of the intermediate equipment.
2. A DCE may perform other functions that are usually performed at the network end of the line.

datagram. (1) In packet switching, a self-contained packet, independent of other packets, that carries information sufficient for routing from the originating data terminal equipment (DTE) to the destination DTE without relying on earlier exchanges between the DTEs and the network. (l) (2) In TCP/IP, the basic unit of information passed across the Internet environment. A datagram contains a source and destination address along with the data. An Internet Protocol (IP) datagram

consists of an IP header followed by the transport layer data. See also *packet* and *segment*. (3) A particular type of information encapsulation, at the network layer of the adapter protocol. No explicit acknowledgment for the information is sent by the receiver. Transmission relies on the best effort of the link layer. See also *best-effort delivery*.

Datagram Delivery Protocol (DDP). An AppleTalk base protocol that provides network connectivity by means of connectionless socket-to-socket delivery service on the internet layer.

data link connection identifier (DLCI). A numeric identifier that is used in a frame-relay network to identify the next segment of a permanent virtual circuit over which a frame is to be relayed. The following table, excerpted from American National Standards Institute (ANSI) Standard T1.618, indicates the functions associated with certain DLCI values:

DLCI Values	Function
0	in-channel signaling
1 – 15	reserved
16 – 991	assigned using frame-relay connection procedures
992 – 1007	layer 2 management of frame-relay bearer service
1008 – 1022	reserved
1023	in-channel layer management

data link control (DLC). A set of rules used by nodes on a data link (such as an SDLC link or a token ring) to accomplish an orderly exchange of information.

data link control (DLC) layer. In SNA, the layer that consists of the link stations that schedule data transfer over a link between two nodes and performs error control for the link. Examples of data link control are SDLC for serial-by-bit link connection and data link control for the System/370 channel.

Note: The DLC layer is usually independent of the physical transport mechanism and ensures the integrity of data that reaches the higher layers.

data link level. (1) In the hierarchical structure of a data station, the conceptual level of control or processing logic between high level logic and the data link that maintains control of the data link. The data link level performs such functions as inserting transmit bits and deleting receive bits; interpreting address and control fields; generating, transmitting, and interpreting commands and responses; and computing and interpreting frame check sequences. (2) In X.25 communications, synonym for *frame level*.

data link switching. A method of transporting network protocols that use Institute of Electrical and Electronics Engineers (IEEE) 802.2 logical link control (LLC) type 2. Systems Network Architecture (SNA) and NetBIOS are examples of protocols that use LLC type 2.

data network. An arrangement of data circuits and switching facilities for establishing connections between data terminal equipment (DTE). (I)

data packet. In X.25 communications, a packet used for the transmission of user data on a virtual circuit at the DTE/DCE interface.

data service unit (DSU). A device that provides a digital data service interface directly to the data terminal equipment (DTE). The primary function of the DSU is to convert the binary data pulse received from the DTE into bipolar line coding used on the telecommunications line. The DSU also performs clocking, signal regeneration, and equalization of the channel. See *channel service unit (CSU)*.

data stream. A continuous stream of data elements being transmitted, or intended for transmission, in character or binary-digit form, using a defined format.

data terminal equipment (DTE). That part of a data station that serves as a data source, data sink, or both. (I) (A)

data terminal ready (DTR). A signal to the modem used with the EIA 232 protocol.

data transfer rate. The average number of bits, characters, or blocks per unit time passing between corresponding equipment in a data transmission system. (I)

Notes:

1. The rate is expressed in bits, characters, or blocks per second, minute, or hour.
2. Corresponding equipment should be indicated; for example, modems, intermediate equipment, or source and sink.

DCE. Data circuit-terminating equipment.

DCE clear confirmation packet. A call supervision packet that a data circuit-terminating equipment (DCE) transmits to confirm that a call has been cleared.

DDP. Datagram Delivery Protocol.

DECnet. A network architecture that defines the operation of a family of software modules, databases, and hardware components typically used to tie Digital Equipment Corporation systems together for resource sharing, distributed computation, or remote system configuration. DECnet network implementations follow the Digital Network Architecture (DNA) model. The IBM 6611 Network Processor supports DECnet Phase IV and DECnet Phase IV-Prime.

default route. A route, in a routing table, that is used when no other route is specified or appropriate.

demon. Synonym for *daemon*.

designated router. A router that informs end nodes of the existence and identity of other routers. The selection of the end node is based upon the router with the highest priority. When several routers share the highest priority, the router with the highest station address is selected.

destination node. The node to which a request or data is sent.

destination service access point (DSAP). In SNA and TCP/IP, a logical address that allows a system to route data from a remote device to the appropriate communications support. See *source service access point (SSAP)*.

detailed data. Short strings of textual data transported in a network management vector transport and displayed, without any interpretation or translation, by a problem management focal-point program.

device. (1) An input/output unit such as a terminal, display, or printer. (2) A physical entity attached to the network that requires data transportation service.

diagnostics. The process of investigating the cause or nature of a condition or a problem in a product or system.

digital. (1) Pertaining to data that consists of digits. (T) (2) Pertaining to data in the form of digits. (A) (3) Contrast with *analog*.

directory. A table of identifiers and references to the corresponding items of data. (I) (A)

disable. To make nonfunctional.

disabled. (1) Pertaining to a state of a processing unit that prevents the occurrence of certain types of interruptions. (2) Pertaining to the state in which a transmission control unit or audio response unit cannot accept incoming calls on a line. (3) Nonoperational or nonfunctional.

discarded packet. A packet that cannot be delivered because of congestion and resource constraints on the system.

distributed directory database. The complete listing of all the resources in the network as maintained in the individual directories scattered throughout an APPN network. Each node has a piece of the complete directory, but it is not necessary for any one node to have the entire list. Entries are created, modified, and deleted through system definition, operator action, automatic registration, and ongoing network search procedures.

DLC. Data link control.

DLCI. Data link connection identifier.

DNS. Domain name system.

domain. (1) In the Internet, a part of a naming hierarchy in which the domain name consists of a sequence of names (labels) separated by periods (dots). (2) In Open Systems Interconnection (OSI), an administrative partition of a complex distributed system. (3) That part of a computer network in which the data processing resources are under common control. (T)

domain name system (DNS). The online distributed database system used to map machine names to Internet Protocol (IP) addresses.

dotted decimal notation. The syntactical representation for a 32-bit integer that consists of four 8-bit numbers written in base 10 with periods (dots) separating them. It is used to represent addresses in the Internet.

DSAP. Destination service access point.

DSU. Data service unit.

DTE. Data terminal equipment. (A)

DTR. Data terminal ready.

dump. (1) To copy the contents of all or part of virtual storage for the purpose of collecting error information. (2) Data that have been dumped. (T)

E

EBCDIC. Extended binary-coded decimal interchange code. A coded character set consisting of 8-bit coded characters. (A)

echo. In data communication, a reflected signal on a communications channel. On a telecommunications terminal, each signal is displayed twice, once when entered at the local terminal and again when returned over the communications link. This allows the signals to be checked for accuracy.

EGP. Exterior Gateway Protocol.

EIA. Electronic Industries Association.

EIA 232. In data communications, a specification of the Electronic Industries Association (EIA) that defines the interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE), using serial binary data interchange.

EIA 422. In data communications, a specification of the Electronic Industries Association (EIA) that defines the electrical characteristics for balanced voltage digital interface circuits for the interchange of serial binary data between data terminal equipment (DTE) and data circuit-terminating equipment (DCE), or any

point-to-point interconnection of serial binary signals between digital equipment. The international equivalent is CCITT Recommendation V.11.

Electronic Industries Association (EIA). An organization of electronics manufacturers that advances the technological growth of the industry, represents the views of its members, and develops industry standards.

EN. End node.

enable. To make functional.

enabled. (1) On a LAN, pertaining to an adapter or device that is active, operational, and able to receive frames from the network. (2) Pertaining to a state of a processing unit that allows the occurrence of certain types of interruptions. (3) Pertaining to the state in which a transmission control unit or an audio response unit can accept incoming calls on a line.

encapsulation. A technique used by layered protocols by which a layer adds header information to the protocol data unit (PDU) from the layer above.

end node (EN). (1) A node that is usually attached to a single data link and does not perform routing functions. It is possible, however, for a routing node with a single line to be an end node. (2) See *Advanced Peer-to-Peer Networking (APPN) end node* and *low-entry networking (LEN) end node*

ER. (1) Explicit route. (2) Exception response.

Ethernet. (1) A 10-Mbps baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by collision detection and transmission. Ethernet uses carrier sense multiple access with collision detection (CSMA/CD). (2) A passive coaxial cable whose interconnections contain devices or components, or both, that are all active. It uses CSMA/CD technology to provide a best-effort delivery system.

Ethernet network. A baseband LAN with a bus topology in which messages are broadcast on a coaxial cable using the carrier sense multiple access with collision detection (CSMA/CD) transmission method.

exception. An abnormal condition such as an I/O error encountered in processing a data set or a file.

exception response (ER). In SNA, a protocol requested in the form-of-response-requested field of a request header (RH) that directs the receiver to return a response only if the request is unacceptable as received or cannot be processed; that is, a negative response, but not a positive response, may be returned.

explicit route (ER). In SNA, a series of one or more transmission groups that connect two subarea nodes. An explicit route is identified by an origin subarea address, a destination subarea address, an explicit route number, and a reverse explicit route number. Contrast with *virtual route (VR)*.

explorer frame. See *explorer packet*.

explorer packet. A packet, generated by the source host that traverses the entire token-ring network gathering information on the possible paths the host might use.

extended binary-coded decimal interchange code (EBCDIC). A coded character set consisting of 256 8-bit characters.

exterior gateway. A gateway on one autonomous system that communicates with another autonomous system. An interior gateway communicates only with its own autonomous system.

Exterior Gateway Protocol (EGP). An Internet Protocol (IP) routing protocol, used between domains and autonomous systems, that allows for network reachability information to be advertised and exchanged. IP network addresses in one autonomous system are advertised to another autonomous system by means of EGP-participating routers.

F

fast select. (1) An option of a virtual call facility that allows inclusion of data in call-setup and call-clearing packets. (I) (2) In X.25 communications, an optional facility that allows inclusion of data in call request and clear request packets.

field replaceable unit (FRU). An assembly that is replaced in its entirety when any one of its components fails. In some cases a field replaceable unit may contain other field replaceable units.

File Transfer Protocol (FTP). The Internet protocol (and program) used to transfer files between hosts. It is an application layer protocol in TCP/IP that uses TCP and TELNET protocols to transfer bulk-data files between machines or hosts.

filter. (1) A device or program that separates data, signals, or material in accordance with specified criteria. (A) (2) A singular filter identifies a host, subnet, or all hosts with a single expression. A dual filter identifies two end points from which to deny or allow traffic. (3) See also *sliding window filter*.

flow control. In SNA, the process of managing the rate at which data traffic passes between components of the network. The purpose of flow control is to optimize the flow rate of message units with minimum congestion in the network; that is, to neither overflow the buffers at the receiver or at intermediate routing nodes, nor leave the receiver waiting for more message units.

focal point (FP). (1) See *management services focal point*. (2) An entry point that provides centralized management and control for other entry points for one or more network management categories.

FP. Focal point.

fragment. An Internet datagram containing only a portion of the user data from a larger IP datagram. See also *fragmentation*.

fragmentation. The process of breaking down an Internet datagram into smaller parts to match the capabilities of the physical medium over which it will be transmitted. See also *fragment*.

frame. (1) A packet that is transmitted over a serial line or LANs. See also *packet*. (2) The unit of transmission in some local area networks including the IBM Token-Ring Network. It includes delimiters, control characters, information, and checking characters. (3) In SDLC, the vehicle for every command, every response, and all information that is transmitted using SDLC procedures. (4) In Open Systems Interconnection architecture, a data structure pertaining to a particular area of knowledge and consisting of slots that can accept the values of specific attributes and from which inferences can be drawn by appropriate procedural attachments. (T)

frame level. See *link level*.

frame relay. (1) An interface standard describing the boundary between a user's equipment and a fast-packet network. In frame-relay systems, flawed frames are discarded; recovery comes end-to-end rather than hop-by-hop. (2) A technique derived from the integrated services digital network (ISDN) D channel standard. It assumes that connections are reliable and dispenses with the overhead of error detection and control within the network.

frequency. The rate of signal oscillation, expressed in hertz.

FRU. Field replaceable unit.

FTP. File Transfer Protocol.

full wildcard character. A character that substitutes for all characters.

G

gateway. (1) A node that attaches two or more networks and routes data packets to their destination between those networks. Contrast with *bridge* and *router*. (2) The original Internet term for router or Internet router. (3) A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures. (T)

H

header. (1) System-defined control information that precedes user data. (2) The portion of a message that contains control information for the message such as one or more destination fields, name of the originating station, input sequence number, character string indicating the type of message, and priority level for the message.

Hello. An Internet protocol used by a group of cooperating, trusting routers to allow them to discover minimal delay routes.

hello. A message used by the automatic single-route broadcast function of IBM bridge programs to detect what bridges enter and leave the network and to cause single-route broadcast parameters to be reset accordingly. The root bridge sends a hello message on the network every 2 seconds.

hierarchy. The resource types, display types, and data types that make up the organization, or levels, in a network.

hop. (1) To the routing layer, the logical distance between two nodes in a network. (2) In APPN, a portion of a route that has no intermediate nodes. It consists of only a single transmission group connecting adjacent nodes.

hop count. (1) A metric or measure of distance between two points in an internet. (2) The number of routers or bridges that separate the source from the destination node. (3) In SNA, a measure of the number of links to be traversed in a path to a destination. (4) The number of networks or subnetworks through which a packet passes on the way to its destination.

host. In Internet terminology, an end system.

I

ICMP. Internet Control Message Protocol.

IEEE. Institute of Electrical and Electronics Engineers.

I frame. Information frame.

IGP. Interior Gateway Protocol.

inbound filter. A filter applied to frames flowing into a port from a transmission link or LAN.

incoming call packet. A call supervision packet transmitted by a data circuit-terminating equipment (DCE) to inform a called data terminal equipment (DTE) that another DTE has requested a call.

information (I) frame. A frame in I format used for numbered information transfer.

i-node. In the AIX operating system, the internal structure that describes the individual files in the operating system: there is one i-node for each file. An i-node contains the node, type, owner, and location of a file. The table of i-nodes is stored near the beginning of the file system.

inoperative. The condition of a resource that was active, but is not currently active. The resource could have failed or could have been suspended while a reactivate command was being processed.

input/output channel. In a data processing system, a functional unit that handles transfer of data between internal and peripheral equipment. (I) (A)

insert. To make an attaching device an active part of the LAN.

instance. In object-oriented programming, a member of a class. An instance is therefore the same as an object.

interface. (1) A shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics, as appropriate. The concept includes the specification of the connection of two devices having different functions. (T) (2) Hardware, software, or both, that links systems, programs, or devices.

Interior Gateway Protocol (IGP). Any protocol used to propagate network reachability and routing information within an autonomous system. Examples of IGPs are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

intermediate node. A node that is at the end of more than one branch. (T)

International Organization for Standardization (ISO).

An organization of national standards bodies from various countries established to promote development of standards to facilitate international exchange of goods and services, and develop cooperation in intellectual, scientific, technological, and economic activities.

International Telephone and Telegraph Consultative Committee (CCITT). An international organization that defines technical standards for the interconnection of telephone equipment and internationally controls related aspects of analog and digital communications.

internet. A collection of networks interconnected by a set of routers which allow them to function as a single, large virtual network. See also Internet.

Internet. The largest internet in the world, consisting of large national backbone networks and many regional and campus networks all over the world. The Internet uses the Internet protocol suite.

Internet address. A 32-bit address assigned to hosts using TCP/IP.

Internet Control Message Protocol (ICMP). The protocol used to handle errors and control messages in the Internet Protocol layer. Reports of problems and incorrect datagram destinations are returned to the original datagram source. ICMP is part of the Internet Protocol.

Internet Packet Exchange (IPX). The routing protocol used to connect Novell's servers or any workstation or router that implements IPX with other workstations. Although similar to TCP/IP, it uses different packet formats and terminology. See also *TCP/IP* and *Xerox Network Services (XNS)*.

Internet Protocol (IP). (1) A protocol that routes data through a network or interconnected networks. IP acts as an intermediary between the higher protocol layers and the physical network. This protocol, however, does not provide error recovery, flow control, or guarantee the reliability of the physical network. IP is a connectionless protocol. (2) A protocol used to route data from its source to its destination in an Internet environment.

Inverse Address Resolution Protocol (ARP). A method for discovering a protocol address through the known hardware address. In a frame relay context, the data link connection identifier (DLCI) is synonymous with the known hardware address.

IP. Internet Protocol.

IP address. A 32-bit address assigned to devices or hosts in a TCP/IP internet that maps to a physical address. The IP address is composed of a network and host portion.

IP datagram. The fundamental unit of information passed across the Internet. It contains source and destination addresses along with data and a number of fields that include information such as the length of the datagram, the header checksum, and flags to say whether the datagram can be (or has been) fragmented.

IPX. Internet Packet Exchange.

ISO. International Organization for Standardization.

K

Kbps. Kilobits per second.

keepalive. A message sent among the BGP neighbors to ensure the vitality of the session.

L

LAN. Local area network.

LAN adapter. The circuit card within a communicating device (such as a personal computer) that, together with its associated software, enables the device to be attached to a LAN.

LAN segment. (1) Any portion of a LAN (for example, a single bus or ring) that can operate independently, but is connected to other parts of the network by means of bridges. (2) An entire ring or bus network without bridges.

layer. (1) In network architecture, a group of services that is complete from a conceptual point of view, that is one out of a set of hierarchically arranged groups and that extends across all systems that conform to the network architecture. (T) (2) In the Open System Interconnection reference model, one of seven conceptually complete, hierarchically arranged groups of services, functions, and protocols that extend across all open systems. (T) (3) In SNA, a grouping of related functions that are logically separate from the functions of other groups. Implementation of the functions in one layer can be changed without affecting functions in other layers.

LEN. Low-entry networking.

line switching. Synonym for *circuit switching*.

link. (1) The combination of the link connection (the transmission medium) and two link stations, one at each end of the link connection. A link connection can be shared among multiple links in a multipoint or token-ring configuration. (2) The combination of physical media, protocols, and programming that connect devices in a network.

link-attached. Pertaining to devices that are connected to a controlling unit by a data link. Synonymous with *remote*.

link connection. (1) The physical equipment providing two-way communication between one link station and one or more other link stations; for example, a telecommunication line and data circuit-terminating equipment (DCE). Synonymous with *data circuit*. (2) In SNA, the physical equipment providing two-way communication and error correction and detection between one link station and one or more other link stations.

link level. A part of Recommendation X.25 that defines the link protocol used to get data into and out of the network across the full-duplex link connecting the subscriber's machine to the network node. LAP and LAPB are the link access protocols recommended by the CCITT. See *data link level*.

LLC. Logical link control.

local. Pertaining to a device accessed directly without the use of a telecommunication line.

local area network (LAN). (1) Physical network technology that transfers data at high speed over short distances. (2) A network in which devices are connected to one another for communication and that can be connected to a larger network. See also *token ring* and *Ethernet*. (3) A computer network located on a user's premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. (T) (4) Contrast with *wide area network (WAN)* and *metropolitan area network (MAN)*.

local directory database. That set of resources (LUs) in the network known at a particular node. The resources included are all those in the node's domain as well as any cache entries.

locally administered address. In a local area network, an adapter address that the user can assign to override the universally administered address. Contrast with *universally administered address*.

lock. The means by which integrity of data is ensured by preventing more than one user from accessing or changing the same data or object at the same time.

logical channel. In packet mode operation, a sending channel and a receiving channel that together are used to send and receive data over a data link at the same time. Several logical channels can be established on the same data link by interleaving the transmission of packets.

logical channel number. A number that uniquely identifies a logical channel.

logical connection. In a network, devices that can communicate or work with one another because they share the same protocol. See also *physical connection*.

logical link. A pair of link stations, one in each of two adjacent nodes, and their underlying link connection, providing a single link-layer logical connection between the two nodes. Multiple logical links can be distinguished while they share the use of the same physical media connecting two nodes. Examples are 802.2 logical links used on local area network (LAN) facilities and LAP E logical links on the same point-to-point physical link between two nodes. The term logical link also includes the multiple X.25 logical channels that share the use of the access link from a DTE to an X.25 network.

logical link control (LLC). (1) The data link control (DLC) LAN sublayer that provides two types of (DLC) operation. The first type is connectionless service, which allows information to be sent and received without establishing a link. The LLC sublayer does not perform error recovery or flow control for connectionless service. The second type is connection-oriented service, which requires establishing a link prior to the exchange of information. Connection-oriented service provides sequenced information transfer, flow control, and error recovery. (2) A sublayer of the OSI link layer that defines formats and protocols for exchanging frames between LLC sublayers attached to a local area network. It has provisions that ensure that error-free, nonduplicated, properly ordered frames are delivered to the appropriate data-link user. (3) See also *bridge*, *medium access control (MAC)*, and *medium access control (MAC) protocol*.

logical link control (LLC) protocol. In a local area network, the protocol that governs the exchange of transmission frames between data stations independently of how the transmission medium is shared. (T)

Note: The LLC protocol was developed by the IEEE 802 committee and is common to all LAN standards.

logical link control (LLC) protocol data unit. A unit of information exchanged between link stations in different nodes. The LLC protocol data unit contains a destination service access point (DSAP) address, a source service access point (SSAP), a control field, and user data.

logical unit (LU). A type of network accessible unit that enables end users to gain access to network resources and communicate with each other.

low-entry networking (LEN). A capability in nodes allowing them to directly attach to one another using peer-to-peer protocols and to support multiple and parallel sessions between logical units. However, LEN

does not provide all of the capabilities of APPN; for example, it does not provide CP-CP session support.

low-entry networking (LEN) end node. An end node that provides all SNA end-user services, can attach directly to other nodes using peer protocols, and derives network services implicitly from an adjacent network node when attached to an APPN network without a session between its local control point (CP) and another CP. A LEN end node can also attach to a subarea network as a peripheral node that can support a combination of independent and dependent LUs, but does not support CP-CP sessions for parallel transmission groups.

low-entry networking (LEN) node. A node that supports independent logical unit (LU) protocols, but does not support CP-CP sessions. It may be a peripheral node attached to a boundary node in a subarea network, an end node attached to an APPN network node in an APPN network, or a peer-connected node directly attached to another LEN node or APPN end node. See *low-entry networking (LEN) end node*.

M

MAC. Medium access control.

MAN. Metropolitan area network.

Management Information Base (MIB). (1) A collection of objects that can be accessed by means of a network management protocol. (2) A single standard for network management data that specifies the data items a host or gateway must keep and the operations allowed on each.

management services (MS). Services that assist in the management of networks in areas such as problem management, performance and accounting management, configuration management, and change management.

management services focal point (MSFP). For any given management services discipline (for example, problem determination or response time monitoring), the control point that is responsible for that type of network management data for a sphere of control. This responsibility may include collecting, storing, or displaying the data for all of these. (For example, a problem determination focal point is a control point that collects, stores, and displays problem determination data.)

management station. The system responsible for managing all, or a portion of, a network. The management station communicates with network management agents that reside in the managed node by means of a network management protocol such as Simple Network Management Protocol (SNMP). Synonymous with *network management station (NMS)*.

mapping. The process of relating internet addresses to physical addresses in the network.

mask. To use a pattern of characters to control retention or elimination of portions of another pattern of characters. (I) (A)

maximum transmission unit (MTU). The largest possible unit of data that can be sent on a given physical medium in a single frame. For example, the MTU for Ethernet is 1500 bytes.

Mbps. Megabits per second.

medium access control (MAC). (1) The sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control sublayer. The MAC sublayer includes the medium access port. See *logical link control (LLC)*. (2) For local area networks, the method of determining which device has access to the transmission medium at any one time.

medium access control (MAC) procedure. In a local area network, the part of the protocol that governs access to the transmission medium independently of the physical characteristics of the medium, but takes into account the topological aspects of the network, in order to enable the exchange of data between data stations.

medium access control (MAC) protocol. In a local area network, the protocol that governs access to the transmission medium, taking into account the topological aspects of the network, in order to enable the exchange of data between data stations. (T) See also *logical link control (LLC) protocol*.

medium access control (MAC) sublayer. In a local area network, the part of the data link layer that applies a medium access method. The MAC sublayer supports topology-dependent functions and uses the services of the physical layer to provide services to the logical link control sublayer. (T)

metric. A value, associated with a route, which is used to discriminate between multiple exit or entry points to the same autonomous system. The route with the lowest metric is preferred.

metropolitan area network (MAN). A network formed by the interconnection of two or more networks that may operate at higher speed than those networks, may cross administrative boundaries, and may use multiple access methods. (T) Contrast with *local area network (LAN)* and *wide area network (WAN)*.

MIB. (1) MIB module. (2) Management Information Base.

MIB module. A collection of objects relating to a common management area. See also *Management Information Base (MIB)* and *MIB object*.

MIB object. A data object contained in the Management Information Base (MIB). Synonymous with *MIB variable*.

MIB tree. The structure of the Management Information Base (MIB).

MIB variable. A data object contained in the Management Information Base (MIB). It refers to a specific instance of a specific data object in a MIB module. Synonym for *MIB object*.

MIB view. The collection of managed objects, known to the agent, that is visible to a particular community.

MILNET. The military network that was originally part of ARPANET. It was partitioned from ARPANET in 1984. MILNET provides a reliable network service for military installations.

modem (modulator/demodulator). (1) A functional unit that modulates and demodulates signals. One of the functions of a modem is to enable digital data to be transmitted over analog transmission facilities. (T) (A) (2) A device that converts digital data from a computer to an analog signal that can be transmitted over a telecommunication line, and converts the analog signal received to data for the computer.

modulo. Pertaining to a modulus; for example, 9 is equivalent to 4 modulo 5. See also *modulus*.

modulus. A number, such as a positive integer, in a relationship that divides the difference between two related numbers without leaving a remainder; for example, 9 and 4 have a modulus of 5 ($9-4=5$; $4-9=-5$; and 5 divides both 5 and -5 without leaving a remainder).

monitor. (1) A device that observes and records selected activities within a data processing system for analysis. Possible uses are to indicate significant departures from the norm, or to determine levels of utilization of particular functional units. (T) (2) Software or hardware that observes, supervises, controls, or verifies operations of a system. (A) (3) In a token-ring network, the function required to initiate the transmission of a token on the ring and to provide soft-error recovery in case of lost tokens, circulating frames, or other difficulties. The capability is present in all ring stations.

MS. Management services.

MTU. Maximum transmission unit.

multicast. A special form of broadcast where copies of a packet are delivered to only a subset of all possible destinations. Contrast with *broadcast*.

Multiprotocol Network Program. The IBM software that controls the functions of the IBM 6611 Network

Processor. It is a licensed program made up of base code, the System Manager, and the Configuration Program.

N

Name Binding Protocol (NBP). An AppleTalk protocol that provides name translation function from the AppleTalk entity (resource) name (character string) into an AppleTalk internet address (16-bit number) on the transport layer.

name resolution. The process of mapping a machine name into the corresponding IP address. See also *domain name system (DNS)*.

name server. A station on an internet that translates host names to their respective internet addresses when requested by the stations on the network.

NBP. Name Binding Protocol.

NCP. Network Control Program.

neighbor. A peer gateway acquired by the exterior gateway. Exterior gateways do not communicate with other gateways. Instead, they acquire neighbors through which they communicate.

NetBIOS. Network Basic Input/Output System. The standard interface to networks, IBM personal computers (PCs), and compatible PCs, used on LANs to provide message, print server, and file server functions. The IBM NetBIOS application program interface (API) provides a programming interface to the LAN so that an application program can have LAN communication without knowledge and responsibility of the data link control (DLC) interface.

network. (1) A configuration of data processing devices and software connected for information interchange. (2) An arrangement of nodes and connecting branches. (T) (3) A group of nodes and the links interconnecting them. (4) An interconnected group of nodes. (5) The interconnection of two or more subnets.

network address. See *Internet address*.

network architecture. The logical structure and operating principles of a computer network. (T)

Note: The operating principles of a network include those of services, functions, and protocols.

network congestion. An undesirable overload condition caused by traffic in excess of what a network can handle.

network identifier (ID). A 1- to 8-byte customer-selected name or an 8-byte IBM-registered name that uniquely identifies a specific subnetwork.

network interface (NI). The point of interconnection between the public switched network and a privately owned terminal.

network layer. In Open Systems Interconnection (OSI), the layer that is responsible for routing, switching, and link-layer access across the entire OSI environment.

network management. The process of planning, organizing, and controlling a communication-oriented data processing or information system.

network management agent. A function that resides in a workstation, server, or router that is specified as a managed node. The agent provides network management information to the network management station.

network management station (NMS). The system responsible for managing a network or a portion of a network. The NMS communicates with network management agents, which reside in the managed nodes, by means of a network management protocol. See also *agent*.

network manager. A program or group of programs that monitor, manage, and diagnose the problems of a network.

network node (NN). Synonym for *Advanced Peer-to-Peer Networking (APPN) network node*.

network operator. (1) A person or program responsible for controlling the operation of all or part of a network. (2) In a multiple-domain network, a person or program responsible for controlling all domains.

network terminating unit (NTU). In X.25 communications, the point of access to a network.

network user address (NUA). In X.25 communications, the X.121 address containing up to 15 binary code digits.

NI. Network interface.

NMS. Network management station.

NN. Network node.

node. (1) Any device, attached to a network, that transmits and receives data. (2) An endpoint of a link, or a junction common to two or more links in a network. (3) In a network, a point at which one or more functional units connect channels or data circuits. (I)

nonseed router. A router that acquires network number range and zone list information from a seed router attached to the same network. Contrast with *seed router*.

notification. An unscheduled, spontaneously generated event, issued by an object manager when a significant or fatal condition occurs.

NRZ. Non-return-to-reference recording. (I) (A)

NRZI. Non-return-to-zero (inverted) recording. Deprecated term for *non-return-to-zero change-on-ones recording (NRZ-1)*. See also *NRZ-1*.

NRZ-1. Non-return-to-zero change-on-ones recording. (I) (A)

NTU. Network terminating unit.

NUA. Network user address.

O

object. In object-oriented programming, an abstraction consisting of data and the operations associated with that data. See also *class* and *instance*.

object identifier. An administratively assigned data type defined in ASN.1 syntax for an object in a MIB module. It is a unique identifier that is used by SNMP software and the SNMP protocol. See *MIB object*.

octet. A byte that consists of 8 bits. (T)

open. (1) To make an adapter ready for use. (2) A break in an electrical circuit.

Open Shortest Path First (OSPF). A function that provides intra-domain information transfer for the Internet Protocol (IP). An alternative to the Routing Information Protocol (RIP), OSPF allows the lowest-cost routing and handles routing in large regional or corporate networks.

OSPF. Open Shortest Path First.

outbound filter. A filter that is applied to frames flowing out of a port onto a transmission link or LAN.

P

packet. (1) In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals, and possibly error control information are arranged in a specific format. (I) (2) See *call-accepted packet*, *call connected packet*, *call request packet*, *clear indication packet*, *clear request packet*, *data packet*, *DCE clear confirmation packet*, *discarded packet*, *incoming call packet*, *permit packet*, and *reset packet*. See also *frame*.

packet internet groper (PING). A program used in TCP/IP networks to test the ability to reach destinations by sending the destinations an Internet Control

Message Protocol (ICMP) echo request and waiting for a reply.

packet mode operation. Synonym for *packet switching*.

packet modulo. The highest sequence number the packet level uses before resetting the count and beginning the count again.

packet switching. (1) The process of routing and transferring data by means of addressed packets so that the media is occupied only during the transmission of a packet. On completion of the transmission, the media is made available for the transfer of other packets. (l) (2) Synonymous with *packet mode operation*. See *circuit switching*.

page. (1) In a virtual storage system, a fixed-length block that has a virtual address and is transferred as a unit between real storage and auxiliary storage. (l) (A) (2) The information displayed at the same time on the screen of a display device. (3) To replace the information displayed on the screen with prior or subsequent information from the same file.

path. (1) In a network, any route between any two nodes. A path may include more than one branch. (T) (2) The series of transport network components (path control and data link control) that are traversed by the information exchanged between two network accessible units (NAUs). See also *explicit route (ER)*, *route extension (REX)* and *virtual route (VR)*.

path control (PC). The function that routes message units between network accessible units in the network and provides the paths between them. It converts the basic information units (BIUs) from transmission control (possibly segmenting them) into path information units (PIUs) and exchanges basic transmission units containing one or more PIUs with data link control. Path control differs by node type: some nodes (T2.0 and T2.1, for example) use local addresses or session identifiers for routing, and others (subarea nodes) use network addresses for routing.

PC. Path control.

PDU. Protocol data unit.

peer-to-peer. In network architecture, any functional unit that resides in the same layer as another entity.

permit packet. At the interface between a data terminal equipment (DTE) and a data circuit-terminating equipment (DCE), a packet used to transmit permits over a virtual circuit.

physical circuit. A circuit established without multiplexing. See *data circuit*. Contrast with *virtual circuit*.

physical connection. A connection that establishes an electrical circuit.

physical layer. In the Open Systems Interconnection reference model, the layer that provides the mechanical, electrical, functional, and procedural means to establish, maintain, and release physical connections over the transmission medium. (T)

PING. Packet internet groper.

Point-to-Point Protocol (PPP). A protocol that provides router-to-router and host-to-host network connections over both synchronous and asynchronous circuits.

poison reverse. A technique for minimizing network convergence. After a connection disappears, the router advertising the connection retains the routing table entry for several update periods, and specifies an infinite cost in its broadcasts.

polling. (1) Interrogation of devices for purposes such as to avoid contention, to determine operational status, or to determine readiness to send or receive data. (A) (2) On a multipoint connection or a point-to-point connection, the process whereby stations are invited, one at a time, to transmit. (l)

port. (1) An access point for data entry or exit. (2) A connector on a device to which cables for other devices such as display stations and printers are attached. Synonymous with *socket*. (3) In TCP/IP, a 16-bit number used to communicate between TCP and a higher-level protocol or application. Some protocols, such as File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP), use the same port number in all TCP/IP implementations. (4) The representation of a physical connection to the link hardware. A port is sometimes referred to as an adapter; however, there can be more than one port on an adapter. There may be one or more ports controlled by a single DLC process. (5) An abstraction used by transport protocols to distinguish among multiple destinations within a host machine.

port number. The identification of an application entity to the transport service in IP.

PPP. Point-to-Point Protocol.

preferential closed user group (CUG). In X.25 communications, the default closed user group.

problem determination. The process of determining the source of a problem; for example, a program component, a machine failure, telecommunication facilities, user or contractor-installed programs or equipment, an environment failure such as a power loss, or user error.

processor. In a computer, a functional unit that interprets and executes instructions. A processor consists of at least an instruction control unit and an arithmetic and logic unit. (T)

protocol. (1) A formal description of messages to be exchanged and the rules to be followed when two or more systems communicate. The description can apply to various levels that facilitate communication: physical, machine, application, and transport levels for example. (2) In Open Systems Interconnection architecture, a set of semantic and syntactic rules that determine the behavior of entities in the same layer in performing communication functions. (T) (3) In SNA, the meanings of, and the sequencing rules for, requests and responses used for managing the network, transferring data, and synchronizing the states of network components.

protocol data unit (PDU). A unit of data specified in a protocol of a given layer and consisting of protocol control information of this layer, and possibly user data of this layer. (T)

PU. Physical unit.

R

read-only memory (ROM). Memory in which stored data cannot be modified by the user except under special conditions.

reassembly. The process of putting segmented packets back together after they have been received.

Recognized Private Operating Agency (RPOA). Any individual, company, or corporation, other than a government department or service, that operates a telecommunication service and is subject to the obligations undertaken in the Convention of the International Telecommunication Union and in the Regulations; for example, a communication common carrier.

Recommendation X.21. An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for a general-purpose interface between data terminal equipment and data circuit equipment for synchronous operations on a public data network.

Recommendation X.25. An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for the interface between data terminal equipment and packet-switched data networks. See also *packet switching*.

reduced instruction-set computer (RISC). A computer that uses a small simplified set of frequently used instructions for rapid execution.

remote. Pertaining to a system, program, or device that is accessed in a separate node. Contrast with *local*.

Remote Execution Protocol (REXEC). A protocol that allows the execution of a command or program on any

host in the network. The local host receives the results of the command execution.

remote procedure call (RPC). A facility that a client uses to request the execution of a procedure call from a server. This facility includes a library of procedures and an external data representation.

Request for Comments (RFC). Documents that describe the Internet suite of protocols and related experiments. All Internet standards are written as RFCs.

reset. On a virtual circuit, reinitialization of data flow control. At reset, all data in transit are eliminated.

reset packet. A packet used to reset a virtual circuit at the interface between the data terminal equipment (DTE) and the data circuit-terminating equipment (DCE).

REX. Route extension.

REXEC. Remote Execution Protocol.

RFC. Request for Comments.

ring. See also *ring network*.

ring network. (1) A network configuration in which devices are connected by unidirectional transmission links to form a closed path. (2) A network in which every node has exactly two branches connected to it and in which there are exactly two paths between any two nodes. (T)

ring segment number. The part of the virtual storage ring address needed to refer to a segment.

RIP. Routing Information Protocol.

RISC. Reduced instruction-set computer.

rlogin (remote LOGIN). A service offered by Berkeley UNIX systems that allows authorized users of one machine to connect to other UNIX systems across an internet and interact as if their terminals were connected directly. The rlogin software passes information about the user's environment (for example, terminal type) to the remote machine.

ROM. Read-only memory. (A)

route. The path that network traffic uses to get from source to destination.

route bridge. A function of an IBM bridge program that allows two bridge computers to use a telecommunications link to connect two LANs. Each bridge computer is connected directly to one of the LANs, and the telecommunication link connects the two bridge computers.

route extension (REX). In SNA, the path control network components, including a peripheral link, that make up the portion of a path between a subarea node and a network addressable unit (NAU) in an adjacent peripheral node. See also *explicit route (ER)*, *path*, and *virtual route (VR)*.

router. (1) A computer that determines that path of network traffic flow. The path selection is made from several paths based on information obtained from specific protocols, algorithms that attempt to identify the shortest and/or best path, and other criteria such as metrics or protocol-specific destination addresses. (2) An attaching device that connects two LAN segments, which use similar or different architectures, at the reference model network layer. Contrast with *bridge* and *gateway*. (3) In OSI terminology, a router is a network layer intermediate system.

routing. (1) The assignment of the path by which a message will reach its destination. (2) In SNA, the forwarding of a message unit along a particular path through a network, as determined by the parameters carried in the message unit, such as the destination network address in a transmission header.

Routing Information Protocol (RIP). (1) An IP interior gateway protocol that is used to exchange routing information. It is supplied with and used by Berkeley UNIX systems. (2) A protocol that provides intradomain routing information transfer and calculates a route based upon the least number of hops, regardless of link transmission speed. It is used by several routing protocols including the Internet Protocol (IP), Internet Packet Exchange (IPX), and Xerox Network Services (XNS).

routing protocol. A technique for each router to find another router and to keep up to date about the best way to get to every network. Examples of routing protocols are: Routing Information Protocol (RIP), Hello, and Open Shortest Path First (OSPF).

routing table. A collection of path information, or routes, that is used to direct datagram (packet) forwarding through an internet. The table contains information that is passed among routers to identify network topology and destination feasibility.

Routing Table Maintenance Protocol (RTMP). An AppleTalk protocol that provides routing information generation and maintenance on the transport layer by means of the AppleTalk routing table. The AppleTalk routing table directs packet transmission through the internet from source socket to destination socket.

RPC. Remote procedure call.

RPOA. Recognized Private Operating Agency.

RSB. A variant of the *rlogin* command that invokes a command interpreter on a remote UNIX machine and

passes the command line arguments to the command interpreter, skipping the *rlogin* step completely.

RTMP. Routing Table Maintenance Protocol.

S

SAA. Systems Application Architecture.

SAP. (1) Service Advertising Protocol. (2) Service access point.

SCSI. Small computer system interface.

SDLC. Synchronous Data Link Control.

seed router. A router that maintains configuration data (network range numbers and zone lists, for example) for the network. Each network must have at least one seed router. The seed router must be initially set up using the configurator tool. Contrast with *nonseed routers*.

segment. (1) A section of cable between components or devices. A segment may consist of a single patch cable, multiple patch cables that are connected, or a combination of building cable and patch cables that are connected. (2) The unit of transfer between TCP functions in different machines. Each segment contains control and data fields whereby the current byte stream position and actual data bytes are identified along with a checksum to validate received data.

select. The process of choosing a single symbol or menu item by placing the cursor on it and clicking the mouse button.

sequence number. A number assigned to a particular frame or packet to control the transmission flow and receipt of data.

serial port. On personal computers, a port used to attach devices such as display devices, letter-quality printers, modems, plotters and pointing devices such as light pens and mice; it transmits data one bit at a time.

server. (1) A functional unit that provides shared services to workstations over a network; for example, a file server, a print server, a mail server. (T) (2) A class of adapter in a network node that performs local processing and does not have any physical connections to other devices (as do port adapters and trunk adapters). (3) A device, program, or code module on a network dedicated to providing a specific service to a network. (4) On a LAN, a data station that provides facilities to other data stations. Examples are a file server, print server, and mail server.

service access point (SAP). (1) A logical point made available by an adapter where information can be received and transmitted. A single service access

point can have many links terminating in it. (2) In Open Systems Interconnection (OSI) architecture, the point at which the services of a layer are provided by an entity of that layer to an entity of the next higher layer. (T)

Service Advertising Protocol (SAP). A protocol that provides a mechanism that allows IPX servers on an internet to advertise their services by name and type. Servers using this protocol have their name, service type, and internet address recorded in all file servers running NetWare Version 2.1 (and later). A mechanism is also provided that allows a workstation to broadcast a query to discover the identities of all servers of all types, all servers of a specific type, or the nearest server of a specific type. SAP also provides a mechanism for workstations to query any file server running NetWare to discover the names and addresses of all servers of a specific type.

session. (1) In network architecture, for the purpose of data communication between functional units, all the activities that take place during the establishment, maintenance, and release of a connection. (T) (2) A logical connection between two network accessible units (NAUs) that can be activated, tailored to provide various protocols, and deactivated as requested. Each session is uniquely identified in a transmission header (TH) accompanying any transmissions exchanged during the session. (3) The data transport connection resulting from a call or link between two devices. (4) The period of time during which a user of a node can communicate with an interactive system, usually the elapsed time between logon and logoff.

session activation request. In SNA, a request that activates a session between two network accessible units (NAUs) and specifies session parameters that control various protocols during session activity.

Simple Network Management Protocol (SNMP). (1) An IP network management protocol that is used to monitor routers and attached networks. (2) A TCP/IP-based protocol for exchanging network management information and outlining the structure for communication among network devices. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application's Management Information Base (MIB).

sliding window. A technique, used by protocols when sending a stream of bytes, that allows the sender to transmit up to n (usually around 10) packets before an acknowledgment arrives. After the sender sends an acknowledgment for the first packet, the packet window "slides" along the stream and sends another.

sliding window filter. A filter of variable window length that can be placed anywhere on a frame for scrutiny of the frame.

small computer system interface (SCSI). A hardware interface that enables a variety of peripheral devices to communicate with one another.

SNA. Systems Network Architecture.

SNAP. Subnetwork Access Protocol.

SNMP. Simple Network Management Protocol.

socket. The abstraction provided by the University of California's Berkeley Software Distribution (commonly called Berkeley UNIX or BSD UNIX) that serves as an endpoint for communication between processes or applications.

source route bridging. A bridging method that uses the routing information (RI) field in the IEEE 802.5 medium access control (MAC) header of a frame to determine which rings or token-ring segments the frame must transit. The RI field is inserted into the MAC header by the originating (source) node. The information in the RI field is derived from explorer packets generated by the source host.

source router. The router that determines the route the frame will follow.

source routing. A method by which the sending station determines the route the frame will follow and includes the routing information with the frame. Bridges then read the routing information to determine if they should forward the frame.

source service access point (SSAP). In SNA and TCP/IP, the SSAP is a logical address that allows a system to send data to a remote device from the appropriate communications support. See also *destination service access point (DSAP)*.

spanning tree. In LAN contexts, the method by which bridges automatically develop a routing table and update that table in response to changing topography to ensure that there is only one route between any two LANs in the bridged LAN. This method prevents packet looping, where a packet returns in a circuitous route back to the sending router.

split horizon. A technique for minimizing network convergence. A router records the interface over which it received a particular route and does not propagate its information about the route back over the same interface.

SSAP. Source service access point.

static route. The route between hosts, networks, or both that is manually entered into a routing table.

station. An input or output point of a system that uses telecommunication facilities; for example, one or more systems, computers, terminals, devices, and

associated programs at a particular location that can send or receive data over a telecommunication line.

subarea. A portion of the SNA network consisting of a subarea node, attached peripheral nodes, and associated resources. Within a subarea node, all network accessible units (NAUs), links, and adjacent link stations (in attached peripheral or subarea nodes) that are addressable within a subarea, share a common subarea address, and have distinct element addresses.

subnet. Shortened form of subnetwork. See *subnetwork*.

subnet address. An extension to the basic IP address where a portion of the host address is interpreted as the local network address.

subnet mask. A bit template that identifies to the TCP/IP protocol code the bits of the host address that are to be used for routing for specific subnets.

subnetwork. Any group of nodes that have a set of common characteristics, such as the same network ID.

Subnetwork Access Protocol (SNAP). A 5-byte protocol discriminator that identifies the non-IEEE standard protocol family to which it belongs.

subsystem. A secondary or subordinate system, usually capable of operating independently of, or asynchronously with, a controlling system. (T)

SVC. Switched virtual circuit.

synchronous. (1) Pertaining to two or more processes that depend on the occurrence of specific events such as common timing signals. (T) (2) Occurring with a regular or predictable time relationship. (3) Contrast with *asynchronous*.

Synchronous Data Link Control (SDLC). A discipline conforming to subsets of the Advanced Data Communication Control Procedures (ADCCP) of the American National Standards Institute (ANSI) and High-Level Data Link Control (HDLC) of the International Organization for Standardization, for managing synchronous, code-transparent, serial-by-bit information transfer over a link connection. Transmission exchanges may be duplex or half-duplex over switched or non-switched links. The configuration of the link connection may be point-to-point, multipoint, or loop. (I)

SYNTAX. In network management, the SYNTAX clause in the MIB module defines the abstract data structure that corresponds to a managed object.

system. In data processing, a collection of people, machines, and methods organized to accomplish a set of specific functions. (I) (A)

system configuration. A process that specifies the devices and programs that form a particular data processing system.

System Manager. The IBM Multiprotocol Program, System Manager, is a menu-driven interface that is designed to simplify system management and operation tasks.

Systems Application Architecture (SAA) solution. A set of IBM software interfaces, conventions, and protocols that provide a framework for designing and developing applications that are consistent across systems.

Systems Network Architecture (SNA). The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of, networks.

Note: The layered structure of SNA allows the ultimate origins and destinations of information, that is, the end users, to be independent of and unaffected by the specific SNA network services and facilities used for information exchange.

T

TCP. Transmission Control Protocol.

TCP/IP. Transmission Control Protocol/Internet Protocol.

TELNET. (1) The TCP/IP protocol that provides remote terminal connection service. (2) The virtual terminal protocol in the Internet suite of protocols. It allows users of one host to log onto a remote host and interact as directly-attached terminal users of that host.

threshold. (1) In IBM bridge programs, a value set for the maximum number of frames that are not forwarded across a bridge due to errors, before a "threshold exceeded" occurrence is counted and indicated to network management programs. (2) An initial value from which a counter is decremented to 0, or a value to which a counter is incremented or decremented from an initial value.

timeout. (1) An event that occurs at the end of a predetermined period of time that began at the occurrence of another specified event. (I) (2) A time interval allotted for certain operations to occur: for example, response to polling or addressing before system operation is interrupted and restarted.

token. (1) A sequence of bits passed from one ring station to another on a token-ring network that signifies permission to transmit over the network. It consists of a starting delimiter, an access control field, and an end delimiter. The access control field contains a bit that indicates to a receiving station that the token is ready to accept information. If a station has data to send

along the network, it appends the data to the token. When data is appended, the token then becomes a frame. See also *frame*. (2) In a local area network, the symbol of authority passed successively from one data station to another to indicate the station temporarily in control of the transmission medium. Each data station has an opportunity to acquire and use the token to control the medium. A token is a particular message or bit pattern that signifies permission to transmit. (T)

token ring. (1) Network technology that controls media access by passing a token (special packet or frame) between media-attached stations. (2) A network with a ring topology that passes tokens from one attaching ring station (node) to another. See also *local area network (LAN)*.

token-ring network. (1) A ring network that allows unidirectional data transmission between data stations, by a token passing procedure, such that the transmitted data return to the transmitting station. (T) (2) A network that uses a ring topology, in which tokens are passed in a sequence from node to node. A node that is ready to send can capture the token and insert data for transmission. (3) A group of interconnected token rings.

topology. The physical or logical arrangement of nodes in a network. Examples are ring topology and bus topology.

trace. (1) A record of the execution of a computer program. It exhibits the sequences in which the instructions were executed. (A) (2) A record of the frames and bytes transmitted on a network.

Transmission Control Protocol (TCP). (1) A communications protocol used in Internet and in any network that follows the U.S. Department of Defense standards for internetworking protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It assumes that the Internet Protocol is the underlying protocol. (2) A transport protocol in the Internet suite of protocols that provides reliable, connection-oriented, full-duplex data stream service.

Transmission Control Protocol/Internet Protocol (TCP/IP). A set of communication protocols that support peer-to-peer connectivity functions for both local and wide area networks.

transparent bridging. A method for tying individual local area networks (LANs) together through the medium access control (MAC) level. A transparent bridge keeps the tables that hold MAC addresses so that frames seen by the bridge can be forwarded to another LAN if the tables indicate to do so.

trap. Data sent by an SNMP managed node (agent function) to a management station to report an exception condition.

trusted router. A router that can supply what is considered, by other routers in the network, valid routing information and network destination feasibility information.

T1. (1) In the U.S., a 1.544 Mbps public access line. It is available in 24 64 Kbps channels. (2) The European version (E1) transmits at 2.048 Mbps. (3) The Japanese version (J1) transmits at 1.544 Mbps.

U

UDP. User Datagram Protocol.

universally administered address. In a local area network, the address permanently encoded in an adapter at the time of manufacture. All universally administered addresses are unique. Contrast with *locally administered address*.

UNIX (trademark of UNIX Systems Laboratories, Inc.) operating system. An operating system developed by Bell Laboratories that features multiprogramming in a multiuser environment. The UNIX operating system was originally developed for use on minicomputers, but has been adapted for mainframes and microcomputers.

Note: The AIX operating system is IBM's implementation of the UNIX operating system.

user. A function that utilizes the services provided by the server. A host can be a user and a server at the same time. See *client*.

User Datagram Protocol (UDP). (1) In TCP/IP, a packet-level protocol built directly on the Internet Protocol layer. UDP is used for application-to-application programs between TCP/IP host systems. (2) A transport protocol in the Internet suite of protocols that provides unreliable, connectionless datagram service. (3) The Internet Protocol that enables an application program on one machine or process to send a datagram to an application program on another machine or process. UDP uses the Internet Protocol (IP) to deliver datagrams.

V

variable. In SNMP, a match of an object instance name with an associated value.

version. A separately licensed program, based on an existing licensed program, that usually has significant new code or new function.

V.24. In data communications, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE).

V.28. In data communications, a specification of the CCITT that defines the electrical characteristics for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) at rates below 20 kilobits per second.

V.35. In data communications, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) at various data rates.

virtual circuit. (1) A logical connection established between two data terminal equipments (DTEs). (2) In packet switching, the facilities provided by a network that give the appearance to the user of an actual connection. (T) See also *data circuit*. Contrast with *physical circuit*. (3) In a packet-switching data network, a logical end-to-end transmission channel – as opposed to a physical connection – that connects X.25 users. Virtual circuits allow physical transmission facilities to be shared by many users simultaneously.

virtual link. (1) A point-to-point interface that connects border routers that are separated by a non-backbone transit area. Because area routers are part of the Open Shortest Path First (OSPF) backbone, the virtual link connects the backbone. The virtual links ensure that the OSPF backbone does not become discontinuous. (2) When a gateway records the interface over which it received a particular route and does not propagate its information about that route over the same interface.

virtual route (VR). In SNA, a logical connection:

- Between two subarea nodes that is physically realized as a particular explicit route
- That is contained wholly within a subarea node for intranode sessions.

A virtual route between distinct subarea nodes imposes a transmission priority on the underlying explicit route, provides flow control through virtual route pacing, and provides data integrity through sequence numbering of path information units (PIUs). See also *explicit route (ER)*, *path*, and *route extension (REX)*.

vital product data (VPD). Information that uniquely defines system hardware, software, and microcode elements of a processing system.

VPD. Vital product data.

VR. Virtual route.

W

WAN. Wide area network.

wide area network (WAN). (1) A data communications network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks and national telephone networks. Contrast with *local area network (LAN)* and *metropolitan area network (MAN)* (2) A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. (T)

X

X.21. See *Recommendation X.21*.

X.25. See *Recommendation X.25*.

Xerox Network Services (XNS). The suite of internet protocols developed by the Xerox Corporation. Although similar to TCP/IP protocols, XNS uses different packet formats and terminology. See also *IPX*.

XNS. Xerox Network Services.

Z

ZIP. Zone Information Protocol.

zone. (1) A logical grouping of hosts within the AppleTalk internet. (2) A subset of nodes within an internet.

Zone Information Protocol (ZIP). An AppleTalk protocol that provides zone management service by maintaining a mapping of the zone names and network numbers across the internet on the session layer.

Index

Numerics

6611, IBM

See also individual entries

ASCII terminal 13-2

A

AARP tables, viewing adapter entries 10-17

accept connections only from specific IBM 6611s 3-26

access to other IP nodes

a local IBM 6611 9-6

a remote IBM 6611 9-7

controlling user tasks 9-25

description of 7-30

direct IP attachment 14-12

direct-attached terminal 9-3

extended network configurations 9-6

FTP transfer method 14-14

IP network connection 9-7

local access configurations 9-2

logging in to an IBM 6611 9-23

modem 9-17

modem transfer method 14-12

modem-attached terminal 9-5

network-attached terminal 9-4

remote access configurations 9-4

standalone IBM 6611 9-2

through an EIA 232 serial port 9-19

userids and passwords 9-25

using the FTP 10-52

using Xmodem 10-55

viewing user tasks 9-25

accessing the IBM 6611

a local IBM 6611 9-6

a remote IBM 6611 9-7

controlling user tasks 9-25

direct IP attachment 14-12

direct-attached terminal 9-3

extended network configurations 9-6

FTP transfer method 14-14

IP network connection 9-7

local access configurations 9-2

logging in to an IBM 6611 9-23

modem 9-17

modem transfer method 14-12

modem-attached terminal 9-5

network-attached terminal 9-4

remote access configurations 9-4

standalone IBM 6611 9-2

through an EIA 232 serial port 9-19

userids and passwords 9-25

using the FTP 10-52

using Xmodem 10-55

accessing the IBM 6611 (*continued*)

viewing user tasks 9-25

adapter address resolution protocol command

primitives 8-12

adapter and protocol configuration

configuration error message report 14-22

configuration objects 14-7

configuration procedure 14-8

configuration script 14-23

description of 1-2, 7-36

direct IP attachment 14-12

FTP transfer method 14-14

importing and exporting the configuration file 14-17

initial configuration using a diskette 14-11

initial configuration without a diskette 14-11

minimal configuration using System

Manager 14-15

modem transfer method 14-12

port-level list object 14-43

port-level single objects 14-34

reinstating a saved configuration file 14-19

system-level list object 14-50

system-level single objects 14-26

updating configuration parameters 14-4

using configuration information text files 14-20

Adapter and Protocol Configuration menu 7-36

adapter configuration parameters

Ethernet Adapter 5-6

Token-Ring Network 16/4 Adapter 5-3

X.25 adapter 5-30

adapter route tables, viewing 10-9

adapter-dependent parameters

AppleTalk 6-57

DECnet 6-82

description of 6-3

Internet Protocol (IP) 6-51

Internetwork Packet Exchange (IPX) 6-68

NetBIOS 6-50

source route bridging 6-5

source route bridging filters 6-8

Systems Network Architecture (SNA) 6-49

transparent bridging 6-29

transparent bridging filters 6-32

Xerox Network Systems (XNS) 6-75

adding a name server 10-38

adding a time server 10-41

adding a userid 10-33

adding host name to IP address mapping entry 10-36

address

6611

IP network Internet 13-5

address mask 4-18

alerts

enable coldStart trap 4-10

alerts (*continued*)

- enable egpNeighborLoss trap 4-12
- enable enterpriseSpecific trap 4-12
- enable linkDown trap 4-11
- enable linkUp trap 4-11
- enable warmStart trap 4-10
- enterprise-specific trap throttle time 4-8
- allow fast select 5-43
- allow incoming calls 5-41
- allow outgoing calls 5-41
- allow reverse charging 5-42
- AppleTalk 3-101, 6-57
- apply configuration 4-19
- Apply Software Components 12-12
- Apply Software Updates 12-9
- applying configuration
 - parameters that can be changed dynamically 1-11
 - parameters that restart a IBM 6611 function 1-12
 - parameters that restart the IBM 6611 1-20
- applying configuration changes to configuration database 10-41

APPN

- adjacent node definition 3-36, 3-41
- configuration options 3-32
- data link switching definition 3-36
- introduction 3-32
- IP definition 3-41
- network node configuration 3-34
- tune network node 3-43
- appn parameters 14-33
 - system manager-only parameters 14-33
- area ID, OSPF 3-51
- area maximum cost 3-117
- area maximum hops 3-117
- area type, OSPF 3-52
- ARP tables, adding adapter entries 10-15
- ARP tables, adding system entries 10-14
- ARP tables, clearing adapter 10-17
- ARP tables, deleting adapter entries with hardware address 10-16
- ARP tables, deleting adapter entries with host name 10-17
- ARP tables, deleting system entries 10-15
- ARP tables, managing 10-13
- ARP tables, viewing adapter entries 10-15
- ARP tables, viewing system entries 10-14
- AS number 3-99
- AS number, exports 3-95
- AS path origin, BGP import filters 3-80
- ASCII terminal
 - connecting to 6611 serial port S1 13-2, 13-5
 - for service tasks 13-5
 - use with concurrent diagnostics 13-2, 13-5
 - modem attached 13-5
- AT commands 10-22
- atecho 9-16
- authentication type, OSPF 3-52

- authorization key, OSPF 3-53, 3-56
- auto reboot on error 5-12
- auto-call unit 5-36
- auto-call unit disconnection timeout 5-37
- automated software component installation for multiple IBM 6611s 12-23
- automated software update installation for multiple IBM 6611s 12-21
- automated software update installation for one IBM 6611 12-19
- automating management of software changes 12-19
- autonomous system number, BGP group 3-69
- autonomous system number, BGP import filters 3-78
- autonomous system number, EGP 3-88
- autonomous system path specification, BGP import filters 3-78
- autonomous system path specification, export filters. 3-96
- autoreset value 5-39

B

- baud rate for S1 serial port 4-4
- baud rate for S2 serial port 4-4
- BGP 3-67
- BGP configured neighbor IP address 3-73
- BGP configured neighbor name 3-73
- BGP configured neighbor parameters 3-73
- BGP configured neighbor, default network in 3-75
- BGP configured neighbor, generate default route 3-74
- BGP configured neighbor, hold time 3-76
- BGP configured neighbor, interface IP address 3-74
- BGP configured neighbor, metric out 3-73
- BGP configured neighbor, next hop destination 3-73
- BGP configured neighbor, passive 3-75
- BGP configured neighbor, preference 3-75
- BGP group parameters 3-69
- BGP group, autonomous system number 3-69
- BGP group, default network in 3-71
- BGP group, default network out 3-72
- BGP group, generate default route 3-71
- BGP group, hold time 3-72
- BGP group, interface IP address 3-71
- BGP group, metric out 3-70
- BGP group, next hop destination 3-70
- BGP group, passive 3-71
- BGP group, preference 3-72
- BGP import destination 3-81
- BGP import destination, destination mask 3-82
- BGP import destination, preference 3-82
- BGP import destination, restrict routes 3-82
- BGP import filters 3-77
- BGP import filters, AS path origin 3-80
- BGP import filters, autonomous system number 3-78
- BGP import filters, autonomous system path specification 3-78
- BGP import filters, preference 3-81

- BGP import filters, restrict imports 3-81
- BGP neighbor parameters 3-73
- BGP unconfigured neighbor, IP address 3-76
- BGP unconfigured neighbor, mask 3-77
- BGP unconfigured neighbor, neighbor name 3-77
- BGP, default metric 3-69
- BGP, default preference 3-68
- BGP, enable 3-67
- BGP, enable import filters 3-77
- BGP, generate default route 3-68
- BGP, group name 3-70
- BGP, group type 3-69
- BGP, import name 3-78
- BGP, import route filters 3-78
- BGP, local autonomous system number 3-68
- BGP, unconfigured neighbor 3-76
- BGP, unconfigured neighbor parameters 3-76
- Border Gateway Protocol (BGP) 3-67
- box-level parameters
 - AppleTalk 3-101
 - APPN 3-32
 - data link switching 3-18
 - NetBIOS 3-47
 - source route bridging 3-4
 - transparent bridging 3-10
 - XNS 3-109
- bridge number 3-4
- bridge priority 3-5
- bridging, source route
 - bridge number 3-4
 - bridge priority 3-5
 - designated ring number 3-4
 - enable source route bridging 3-4
 - filter ordering (port level)
 - inbound filters 6-16
 - outbound filters 6-25
 - filter ordering (system level) 3-6
- filters
 - inbound sliding window 6-13
 - outbound sliding window 6-23
- forward delay time 3-5
- hello time 3-5
- introduction 3-4
- maximum age 3-5
- restrictions 3-4
- bridging, spanning tree
 - BPDU maximum age 3-17
 - bridge priority 3-5, 3-16
 - forward delay 3-16
 - forward delay time 3-5
 - hello time 3-5, 3-16
 - maximum age 3-5
- broadcast type 5-5
- broadcast, hello 3-63
- broadcast, RIP 3-58

C

- calling address in incoming call packets 5-41
- CCITT support 5-35
- changing passwords 10-34
- changing the date, time, and time zone 10-27
- changing userids and passwords 10-31
- checksum value, XNS 6-78
- circuit cost 6-82
- Clean Up After a Failed Installation 12-16
- closed user group 5-44
- closed user group index 5-49
- closed user group with OA index 5-49
- codes error and status B-1
- command environment, fast-path
 - 3-digit display command primitive 8-100
 - accessing 8-7
 - adapter debug facility command primitives 8-10
 - address resolution protocol: adapter command primitives 8-12
 - address resolution protocol: system command primitives 8-16
 - bridging debug facility command primitives 8-19
 - configuration command primitives 8-25
 - DECnet debug facility command primitives 8-29
 - diskette command primitives 8-37
 - dump: system command primitives 8-40
 - dump: user process command primitives 8-42
 - entering 7-16
 - error report command primitives 8-43
 - executing the command primitives 8-6
 - fast-path exit command primitives 8-53
 - file management command primitives 8-54
 - getting help 8-8
 - hardware VPD command primitives 8-57
 - host name command primitives 8-60
 - host name to IP address mapping command primitives 8-61
 - install command primitives 8-62
 - name server command primitives 8-66
 - process command primitives 8-68
 - remote access command primitives 8-70
 - returning 7-16
 - route table command primitives 8-73
 - serial port command primitives 8-74
 - shutdown: system command primitives 8-76
 - software lock command primitive 8-78
 - software VPD command primitives 8-79
 - statistic-gathering command primitives 8-81
 - terminal control primitives 8-86
 - time server command primitives 8-87
 - time: system command primitives 8-89
 - trace: system command primitives 8-91
 - trace: user process command primitives 8-94
 - user: system command primitives 8-98
- command primitive
 - aarp_sys_list 8-12
 - adp_dump 8-10

command primitive (*continued*)

adp_line_trc_start 8-10
 adp_name_list 8-10
 adp_read_mem 8-11
 adp_show_regs 8-11
 arp_adp_add_perm_nopub 8-12
 arp_adp_add_perm_pub 8-12
 arp_adp_add_temp_nopub 8-13
 arp_adp_add_temp_pub 8-13
 arp_adp_del_addr 8-13
 arp_adp_del_host 8-14
 arp_adp_flush 8-14
 arp_adp_list 8-14
 arp_hw_type_list 8-16
 arp_sys_add_perm_nopub 8-16
 arp_sys_add_perm_pub 8-16
 arp_sys_add_temp_nopub 8-17
 arp_sys_add_temp_pub 8-17
 arp_sys_del_host 8-17
 arp_sys_list 8-18
 atecho 8-70
 brdg_cfg_info 8-19
 brdg_sap_filter 8-19
 config_app 8-25
 config_com 8-25
 config_err_rpt 8-25
 config_file_run 8-26
 config_list 8-26
 config_reinstate 8-26
 config_rej 8-27
 config_rpt 8-27
 config_script 8-27
 dec_adj 8-29
 dec_area_cost 8-29
 dec_area_hop 8-30
 dec_area_min_cost 8-30
 dec_area_min_hop 8-31
 dec_area_out_adj 8-31
 dec_area_reach 8-32
 dec_circuit 8-32
 dec_cost 8-33
 dec_executor 8-33
 dec_hop 8-33
 dec_min_cost 8-34
 dec_min_hop 8-34
 dec_out_adj 8-34
 dec_reach 8-35
 disk_dwn_files_dos 8-37
 disk_dwn_files_unix 8-37
 disk_format_dos_hi 8-37
 disk_format_dos_low 8-38
 disk_format_unix_hi 8-38
 disk_format_unix_low 8-38
 disk_list_files_dos 8-38
 disk_list_files_unix 8-39
 disk_up_files_dos 8-39
 disk_up_files_unix 8-39
 dump_appn 8-42

command primitive (*continued*)

dump_ex_err_log 8-40
 dump_ex_trc_log 8-40
 dump_ipproto 8-42
 dump_prev_info 8-40
 dump_process 8-42
 dump_system 8-40
 dump_system_format 8-41
 dump_system_trans 8-41
 eondif_sysid 8-28
 err_id_list 8-43
 err_log_trans 8-43
 err_rpt_det 8-43
 err_rpt_eid_det 8-44
 err_rpt_eid_sum 8-44
 err_rpt_etype_det 8-45
 err_rpt_etype_sum 8-45
 err_rpt_hw_det 8-46
 err_rpt_hw_rsc_det 8-46
 err_rpt_hw_rsc_sum 8-47
 err_rpt_hw_sum 8-47
 err_rpt_op_de 8-48
 err_rpt_op_sum 8-48
 err_rpt_seq 8-49
 err_rpt_sum 8-49
 err_rpt_sw_det 8-49
 err_rpt_sw_rsc_det 8-50
 err_rpt_sw_rsc_sum 8-50
 err_rpt_sw_sum 8-51
 err_type_list 8-51
 exit 8-53
 files_clr_all_trans 8-54
 files_clr_one_trans 8-54
 files_list_static 8-54
 files_list_trans 8-55
 files_rename_trans 8-55
 files_view_static 8-55
 files_view_trans 8-56
 ftp 8-70
 host_name_set 8-60
 host_name_show 8-60
 hw_cfg_chg 8-57
 hw_def_list 8-57
 hw_detail 8-57
 hw_diag 8-57
 hw_diag_list 8-58
 hw_install_list 8-58
 hw_rsc_list 8-52
 hw_serial_model 8-58
 hw_sup_list 8-59
 hw_vpd_list 8-59
 install_cleanup 8-62
 install_comp 8-62
 install_fix_list 8-62
 install_not_commit_list 8-63
 install_reinstate_saved_comp 8-63
 install_remove_saved_comp 8-63
 install_sw_list 8-63

command primitive (*continued*)

install_up_trans 8-64
install_upd 8-64
install_upd_commit 8-64
install_upd_reject 8-64
install_verify 8-65
interface_list 8-15
map_host_add 8-61
map_host_del 8-61
map_host_list 8-61
modem_rcv 8-70, 8-74
modem_send 8-71, 8-74
name_serv_add 8-66
name_serv_del 8-66
name_serv_list 8-66
name_serv_start 8-67
name_serv_stop 8-67
ping 8-71
port_list 8-19
proc_command 8-68
proc_info 8-68
proc_list 8-68
proc_stat 8-68
proc_table 8-69
quit 8-53
read_3digit 8-100
rlogin 8-71
route_adp_table 8-73
route_sys_table 8-73
s1_at 8-74
s1_baud 8-75
s2_at 8-75
s2_baud 8-75
seq_num_list 8-52
set_backspace 8-86
set_interrupt 8-86
shutdown_at_ipl 8-76
shutdown_at_noipl 8-76
shutdown_soon_ipl 8-76
shutdown_soon_noipl 8-77
stat_adp_brdg 8-20
stat_adp_con 8-81
stat_adp_lanbr 8-20
stat_adp_pack_traf 8-81
stat_adp_proto 8-82
stat_adp_proto_mon 8-82
stat_filter_con 8-81
stat_inet 8-82
stat_io 8-83
stat_mem_man 8-83
stat_net_con 8-83
stat_route 8-83
stat_socket 8-84
stat_srb_sptree 8-20
stat_srb_sptree_frm 8-21
stat_sys_activity 8-84
stat_sys_lanbr 8-21
stat_sys_lanbr_frm 8-21

command primitive (*continued*)

stat_sys_pack_traf 8-84
stat_sys_proto 8-85
stat_tb_sptree 8-22
stat_tb_sptree_frm 8-22
stat_virt_mem 8-85
sw_dep_list 8-79
sw_files_list 8-79
sw_history 8-79
sw_id 8-79
sw_list 8-80
sw_lock 8-78
sw_prereq 8-80
sw_rsc_list 8-52
sw_upd_list 8-80
telnet 8-72
time_date_set 8-89
time_serv_add 8-87
time_serv_del 8-87
time_serv_list 8-87
time_serv_start 8-88
time_serv_stop 8-88
time_zone_set 8-89
trace_appletk_parm_list 8-94
trace_appletk_start 8-94
trace_appletk_stop 8-94
trace_appn_parm_list 8-94
trace_appn_set_flags 8-95
trace_appn_stop 8-95
trace_brdg_start 8-22
trace_brdg_stop 8-23
trace_brdg_view 8-24
trace_dec_level 8-35
trace_dec_log 8-36
trace_dec_mask 8-36
trace_dec_time 8-36
trace_grp_list 8-91
trace_grp_start 8-91
trace_id_list 8-91
trace_id_start 8-91
trace_ipproto_parm_list 8-95
trace_ipproto_start 8-95
trace_ipproto_stop 8-96
trace_log_trans 8-92
trace_rpt_all 8-92
trace_rpt_id 8-92
trace_snmp_list 8-96
trace_snmp_start 8-96
trace_snmp_stop 8-96
trace_stop 8-93
trace_sys_man_trans 8-97
user_add 8-98
user_del 8-98
user_list 8-98
user_passwd 8-99

command primitives

3-digit display command primitive 8-100
accessing 8-7

command primitives (*continued*)

- adapter debug facility command primitives 8-10
- address resolution protocol: adapter command primitives 8-12
- address resolution protocol: system command primitives 8-16
- bridging debug facility command primitives 8-19
- configuration command primitives 8-25
- DECnet debug facility command primitives 8-29
- diskette command primitives 8-37
- dump: system command primitives 8-40
- dump: user process command primitives 8-42
- entering 7-16
- error report command primitives 8-43
- executing the command primitives 8-6
- fast-path exit command primitives 8-53
- file management command primitives 8-54
- getting help 8-8
- hardware VPD command primitives 8-57
- host name command primitives 8-60
- host name to IP address mapping command primitives 8-61
- install command primitives 8-62
- name server command primitives 8-66
- process command primitives 8-68
- remote access command primitives 8-70
- returning 7-16
- route table command primitives 8-73
- serial port command primitives 8-74
- shutdown: system command primitives 8-76
- software lock command primitive 8-78
- software VPD command primitives 8-79
- statistic-gathering command primitives 8-81
- terminal control primitives 8-86
- time server command primitives 8-87
- time: system command primitives 8-89
- trace: system command primitives 8-91
- trace: user process command primitives 8-94
- user: system command primitives 8-98

command status screens 7-9

Commit Applied Updates (Delete Previous Version) 12-16

committing configuration changes to configuration database 10-42

communities, SNMP 4-13

community access 4-15

community address mask 4-14

community address, SNMP 4-14

community name 4-14

community view name 4-15

Concurrent Hardware Diagnostics

- description of 7-25

Concurrent Hardware Diagnostics menu 7-25

concurrent mode, Diagnostic Program 13-2, 13-5

- modem attached ASCII terminal 13-5
- remote IP workstation 13-5

concurrent mode, Diagnostic Programs

- directly attached ASCII terminal 13-2

configuration

- adding a name server 10-38
- adding a time server 10-41
- adding host name to IP address mapping entry 10-36
- applying configuration changes to configuration database 10-41
- baud rate 10-30
- committing configuration changes to configuration database 10-42
- deleting a name server 10-39
- deleting a time server 10-41
- deleting host name to IP address mapping entry 10-36
- initial 2-13
- line speed 10-30
- listing host name to IP address mapping 10-36
- listing name servers 10-37
- listing time servers 10-40
- rejecting configuration changes to configuration database 10-42
- start using host name service 10-38
- start using time service 10-40
- stop using host name service 10-38
- stop using time service 10-40
- system 10-28
- System Manager 7-35, 7-36, 10-28
- the host name and domain name 10-35

configuration considerations

- parameters that can be changed dynamically 1-11
- parameters that restart a IBM 6611 function 1-12
- parameters that restart the IBM 6611 1-20

configuration diskettes 12-33

Configuration Files and Reports

- description of 7-35

Configuration Files and Reports menu 7-35

configuration hosts 4-18

configuration parameters

- AppleTalk 6-57
- APPN 3-32
- Border Gateway Protocol (BGP) 3-67
- data link switching 3-18
- DECnet 3-115, 6-82
- export filters 3-95
- Exterior Gateway Protocol (EGP) 3-83
- frame relay 5-18
- Hello 3-63
- Internet Protocol (IP) 6-51
- Internetwork Packet Exchange (IPX) 6-68
- NetBIOS 3-47, 6-50
- packet filters 3-92
- port-level source route bridging 6-5
- port-level transparent bridging 6-29
- RIP 3-58
- source route bridging 3-4
- system management 4-3
- system-level 3-3
- Systems Network Architecture (SNA) 6-49

- configuration parameters (*continued*)
 - transparent bridging 3-10
 - userids and passwords 4-16
 - X.25 adapter 5-30
 - Xerox Network Systems (XNS) 6-75
 - XNS 3-109
 - configuration program
 - description of 2-2
 - hardware and software requirements 2-3
 - hardware and software requirements for PS/2 2-5
 - installing on a PS/2 2-5
 - Main Window 2-7
 - starting on a PS/2 2-6
 - starting on a RISC System/6000 2-4
 - using 2-7
 - configuration, adapter
 - configuration error message report 14-22
 - configuration objects 14-7
 - configuration procedure 14-8
 - configuration script 14-23
 - description of 1-2, 7-36
 - direct IP attachment 14-12
 - FTP transfer method 14-14
 - importing and exporting the configuration file 14-17
 - initial configuration using a diskette 14-11
 - initial configuration without a diskette 14-11
 - minimal configuration using System Manager 14-15
 - modem transfer method 14-12
 - port-level list object 14-43
 - port-level single objects 14-34
 - reinstating a saved configuration file 14-19
 - system-level list object 14-50
 - system-level single objects 14-26
 - updating configuration parameters 14-4
 - using configuration information text files 14-20
 - configuration, protocol
 - configuration error message report 14-22
 - configuration objects 14-7
 - configuration procedure 14-8
 - configuration script 14-23
 - description of 1-2, 7-36
 - direct IP attachment 14-12
 - FTP transfer method 14-14
 - importing and exporting the configuration file 14-17
 - initial configuration using a diskette 14-11
 - initial configuration without a diskette 14-11
 - minimal configuration using System Manager 14-15
 - modem transfer method 14-12
 - port-level list object 14-43
 - port-level single objects 14-34
 - reinstating a saved configuration file 14-19
 - system-level list object 14-50
 - system-level single objects 14-26
 - updating configuration parameters 14-4
 - using configuration information text files 14-20
 - configurations 9-2
 - configured neighbor IP address, BGP 3-73
 - configured neighbor parameters, BGP 3-73
 - configuring
 - baud rate for S1 serial port 4-4
 - baud rate for S2 serial port 4-4
 - domain name 4-3
 - EIA 232 serial ports 4-4
 - IBM 6611 host name 4-3
 - lock value 4-5
 - SNMP 4-6
 - system configuration parameters 3-3
 - system management parameters 4-3
 - connection decay interval 3-100
 - connection mode 5-36
 - considerations for configuration
 - parameters that can be changed dynamically 1-11
 - parameters that restart a IBM 6611 function 1-12
 - parameters that restart the IBM 6611 1-20
 - contextual help 7-14
 - contextual help, System Manager 7-3
 - controlling password 4-16
 - controlling userid 4-16
 - controlling userid tasks 9-25
 - controlling users 9-25
 - cost, OSPF 3-53
 - CUG selection facility - basic format 5-43
 - CUG selection facility - extended format 5-43
 - CUG with OA facility - basic format 5-43
 - CUG with OA facility - extended format 5-44
 - cylind serial number 5-10
- ## D
- data encoding 5-11
 - data link protocol 5-9
 - data link switching 3-18
 - accept connections only from specific IBM 6611s 3-26
 - destination cache timeout 3-25
 - enable forwarding of SNA traffic 3-25
 - enable NetBIOS frame forwarding 3-25
 - introduction 3-18
 - IP address of remote IBM 6611 3-26
 - restrictions 3-18
 - virtual ring segment number 3-25
 - data rate select 5-23
 - data rate, token-ring 5-5
 - data terminal ready 5-24
 - data, vital product
 - exporting software 12-40
 - hardware 7-34
 - in the error log 11-5
 - software 7-32, 12-33
 - date and time changes 10-26, 10-27
 - day 4-19
 - DECnet
 - introduction 3-115

- default data link switching IP address for this IBM 6611 3-26
- default metric, BGP 3-69
- default metric, EGP 3-84, 3-86
- default network in, BGP configured neighbor 3-75
- default network in, BGP group 3-71
- default network out, BGP group 3-72
- default preference, BGP 3-68
- default SVC receive packet size 5-39, 5-40
- default SVC transmit packet size 5-40
- defining userids and passwords 10-31
- deleting a host name to IP address mapping entry 10-36
- deleting a name server 10-39
- deleting a time server 10-41
- deleting userids 10-33
- designated ring number 3-4
- destination address mask, SNA 3-29, 3-31
- destination address, IP static routes 3-90
- destination address, SNA 3-29, 3-31
- destination address, XNS static routes 3-114
- destination cache timeout 3-25
- destination frame address for outbound filters 6-19
- destination frame address mask for outbound filters 6-20
- destination frame address mask on SRB port 6-10
- destination frame address on SRB port 6-10
- destination frame filter type, SNA 3-30
- destination host address, XNS 6-75
- destination host value, IPX port 6-72
- destination host value, XNS 6-80
- destination IP address 6-55
- destination IP address for X.25 5-47
- destination IPX address 6-69
- destination MAC address, DECnet 3-27
- destination mask, BGP import destination 3-82
- destination mask, EGP 3-89
- destination mask, exports 3-95
- destination mask, hello 3-65
- destination mask, IP static routes 3-90
- destination mask, RIP 3-60
- destination mask, XNS static routes 3-114
- destination name filter type, NetBIOS 3-49
- destination name, NetBIOS 3-47, 3-49, 3-50
- destination network value, IPX port 6-71
- destination network value, XNS 6-79
- destination socket value, IPX port 6-72
- destination socket value, XNS 6-80
- destination XNS address 6-76
- destination, BGP import destination 3-81
- destination, EGP 3-88
- destination, exports 3-95
- destination, hello 3-65
- destination, RIP import 3-60
- devices
 - diagnostic test list 13-2
- Diagnostic Programs, 6611
 - See also* MAPs

- Diagnostic Programs, 6611 (*continued*)
 - ASCII terminal 13-2
 - concurrent mode 13-2, 13-5
 - remote IP workstation 13-2, 13-5
 - System Manager
 - See also* System hardware diagnostics 13-2
- diagnostic routines
 - concurrent mode 13-2
- diagnostics, concurrent
 - description of 7-25
- dialog screens 7-7
- direct connection, baud rate 10-30
- direction in which the packet is moving 6-85
- directory, static 10-21
- directory, transfer 10-19
- DLCI number, DECnet 6-83
- DLCI number, IP 6-56
- DLCI number, IPX 6-69
- DLCI, source route bridging 6-5
- DLCI, XNS 6-77
- DLCIs assigned to this port 5-20
- DLS
 - accept connections only from specific IBM 6611s 3-26
 - destination cache timeout 3-25
 - enable forwarding of SNA traffic 3-25
 - enable NetBIOS frame forwarding 3-25
 - introduction 3-18
 - IP address of remote IBM 6611 3-26
 - restrictions 3-18
 - virtual ring segment number 3-25
- domain address, SNMP 4-10
- domain name 4-3, 10-34
- domain name servers 10-37
- dynamic configuration
 - parameters that can be changed dynamically 1-11
 - parameters that restart a IBM 6611 function 1-12
 - parameters that restart the IBM 6611 1-20

E

- EGP
 - autonomous system number 3-88
 - default metric 3-84, 3-86
 - destination 3-88
 - destination mask 3-89
 - EGP group name 3-84
 - enable EGP 3-83
 - enable EGP import filters 3-88
 - export default route 3-85, 3-87
 - generate default from this neighbor group 3-86
 - generate default route 3-83
 - generate default routes from this neighbor 3-85
 - import default route 3-85, 3-87
 - local autonomous system number 3-83
 - maximum Active neighbors 3-84
 - maximum initial packet size 3-83

EGP (*continued*)

- minimum hello interval 3-85, 3-87
- minimum polling interval 3-85, 3-87
- neighbor ASN 3-84
- neighbor IP address 3-84
- next hop address or domain name 3-87
- preference 3-83, 3-86, 3-88, 3-89
- restrict 3-88
 - restrict routes 3-89
- EGP group name 3-84
- EIA 232 serial port access 9-19
- EIA 232 serial ports, configuring 4-4
- EIA 232-D 5-22
- EIA 422/449 Serial Adapter 5-9
- EIA serial ports 4-4
- eligible to become a designated router, OSPF 3-55
- enable additional multicast addresses 5-7
- enable authenticationFailure trap 4-11
- enable BGP 3-67
- enable BGP import filters 3-77
- enable coldStart trap 4-10
- enable configuration report saver 5-14
- enable DECnet on this interface 6-82
- enable DECnet router 3-116
- enable EGP 3-83
- enable EGP import filters 3-88
- enable egpNeighborLoss trap 4-12
- enable enterpriseSpecific trap 4-12
- enable forwarding of SNA traffic 3-25
- enable forwarding of spanning tree explorer packets 6-7
- enable frame relay on this port 5-19
- enable hello protocol 3-63
- enable interface, Ethernet Adapter 5-6
- enable interface, SDLC Adapter 5-22
- enable interface, serial adapter 5-10
- enable interface, Token-Ring Network 16/4 Adapter 5-3
- enable IP routing on this port 6-51
- enable IPX router 3-102
- enable IPX routing on this port 6-68
- enable LAN bridging protocol on this port 5-12
- enable link quality monitoring 5-16
- enable linkDown trap 4-11
- enable linkUp trap 4-11
- enable name resolution by remote name servers 4-22
- enable NetBIOS frame forwarding 3-25
- enable OSPF 3-51
- enable PPP on this port 5-16
- enable ring error monitor 5-14
- enable ring parameter server 5-14
- enable RIP 3-58
- enable SNA frame forwarding on this port 6-49
- enable SNMP 4-6
- enable source route bridging 3-4
- enable source route bridging on this port 6-5
- enable time service by remote time servers 4-23

- enable warmStart trap 4-10
- enable X.25 5-32
- enable XNS router, XNS 3-109
- encapsulation method, IPX port 6-68
- encapsulation method, XNS 6-75, 6-76
- encapsulation methods
 - frame relay 5-18
- enterprise-specific trap throttle time 4-8
- error and status codes B-1
- error log
 - warning about erasing 11-5, 11-10
- error log facility
 - overview 11-4
- error message screens 7-3
- error protocol active, XNS 6-76
- Ethernet Adapter parameters
 - compatible protocols 5-6
 - enable additional multicast addresses 5-7
 - enable interface 5-6
 - introduction 5-6
 - locally administered Ethernet MAC address 5-7
 - MAC address 5-6
 - multicast MAC address 5-8
- Ethernet transparent bridging 3-10
- event log drive 5-13
- exiting the System Manager 7-16
- export default route, EGP 3-85, 3-87
- Export Filters
 - AS number 3-95, 3-99
 - destination 3-95
 - destination mask 3-95
 - export selection name 3-95
 - from protocol 3-95
 - metric 3-96
 - restrict 3-96
 - tag 3-99
 - to protocol 3-99
 - type 3-99
- export filters, autonomous system path specification 3-96
- export selection name 3-95
- exporting data 10-43
- extended network configurations 9-6
- Exterior Gateway Protocol
 - autonomous system number 3-88
 - default metric 3-84, 3-86
 - destination 3-88
 - destination mask 3-89
 - EGP group name 3-84
 - enable EGP 3-83
 - enable EGP import filters 3-88
 - export default route 3-85, 3-87
 - generate default from this neighbor group 3-86
 - generate default route 3-83
 - generate default routes from this neighbor 3-85
 - import default route 3-85, 3-87
 - local autonomous system number 3-83
 - maximum Active neighbors 3-84

Exterior Gateway Protocol (*continued*)

- maximum initial packet size 3-83
- minimum hello interval 3-85, 3-87
- minimum polling interval 3-85, 3-87
- neighbor ASN 3-84
- neighbor IP address 3-84
- next hop address or domain name 3-87
- preference 3-83, 3-86, 3-88, 3-89
- restrict 3-88
- restrict routes 3-89

F

facilities control 5-41

fast-path environment

- 3-digit display command primitive 8-100
- accessing 8-7
- adapter debug facility command primitives 8-10
- address resolution protocol: adapter command primitives 8-12
- address resolution protocol: system command primitives 8-16
- bridging debug facility command primitives 8-19
- configuration command primitives 8-25
- DECnet debug facility command primitives 8-29
- diskette command primitives 8-37
- dump: system command primitives 8-40
- dump: user process command primitives 8-42
- entering 7-16
- error report command primitives 8-43
- executing the command primitives 8-6
- fast-path exit command primitives 8-53
- file management command primitives 8-54
- getting help 8-8
- hardware VPD command primitives 8-57
- host name command primitives 8-60
- host name to IP address mapping command primitives 8-61
- install command primitives 8-62
- name server command primitives 8-66
- process command primitives 8-68
- remote access command primitives 8-70
- returning 7-16
- route table command primitives 8-73
- serial port command primitives 8-74
- shutdown: system command primitives 8-76
- software lock command primitive 8-78
- software VPD command primitives 8-79
- statistic-gathering command primitives 8-81
- terminal control primitives 8-86
- time server command primitives 8-87
- time: system command primitives 8-89
- trace: system command primitives 8-91
- trace: user process command primitives 8-94
- user: system command primitives 8-98

field edit screens 7-3

file transfer program

- for the configuration file 2-14

file transfer program (*continued*)

- transferring software changes 12-28, 12-30
- file transfer protocol 9-7
- filter based on checksum, XNS 6-78
- filter based on destination network, IPX port 6-71
- filter based on destination network, XNS 6-79
- filter DECnet address 1 3-120
- filter DECnet address 2 3-121
- filter ID, IP packet filters 3-92
- filter ID, DECnet 3-120, 6-84
- filter ID, IPX 3-103, 3-106, 3-108
- filter ID, IPX port 6-70
- filter ID, SNA 3-28, 3-30
- filter ID, XNS 3-110, 3-111, 3-113, 6-77
- filter IP address 1 3-93
- filter IP address 1, IP port filters 6-54
- filter IP address 2 3-94
- filter IP address 2, IP port filters 6-55
- filter IP, IPX/RIP router 3-105
- filter mask 1, DECnet 3-121
- filter mask 2, DECnet 3-121
- filter on destination host, IPX port 6-72
- filter on destination host, XNS 6-79
- filter on destination socket, IPX port 6-72
- filter on destination socket, XNS 6-80
- filter on packet type, IPX port 6-70
- filter on packet type, XNS 6-78
- filter on source host, IPX port 6-73
- filter on source host, XNS 6-81
- filter on source network, IPX port 6-73
- filter on source network, XNS 6-80
- filter on source socket, IPX port 6-73
- filter on source socket, XNS 6-81
- filter on transport control, IPX port 6-71
- filter on transport control, XNS 6-78
- filter routes from, hello 3-66
- filter routes from, RIP imports 3-61
- filter subnet mask 1 3-93
- filter subnet mask 1, IP port filters 6-55
- filter subnet mask 2 3-94
- filter subnet mask 2, IP port filters 6-55
- filter type for inbound ring number filters 6-12
- filter type for outbound filters 6-18
- filter type on SRB port 6-9, 6-11, 6-12
- filter type, DECnet 3-120
- filter type, IP packet filters 3-93
- filter type, IP port filters 6-54
- filter type, port SRB 6-20
- filter type, SRB port 6-21, 6-22
- filtering mode, IPX 3-103, 3-104, 3-106, 3-107
- filtering mode, IPX port 6-70
- filtering mode, XNS 3-110, 3-111, 3-112, 6-77
- filters, BGP import 3-77
- filters, source route bridging 6-8
- flowchart of System Manager 7-17
- force disconnect timeout 5-29
- forward delay time 3-5

- forward NetBIOS datagram and datagram broadcast message on this port 6-50
- forward NetBIOS frames on this port 6-50
- frame modulo 5-36
- frame relay 5-18
- frame relay parameters
 - compatible protocols 5-18
 - DLCIs assigned to this port 5-20
 - enable frame relay on this port 5-19
 - full enquiry interval 5-19
 - introduction 5-18
 - LMI option 5-19
 - polling interval 5-19
 - restriction 5-18
 - use InARP 5-20
- frame type for inbound ring number filters 6-13
- frame type for outbound filters 6-19
- frame type on SRB port 6-9, 6-11
- frame type, SRB port 6-20, 6-22, 6-28
- frame window size 5-36
- from protocol, exports 3-95
- FTP 10-43, 10-52
 - for the configuration file 2-14
 - transferring software changes 12-28, 12-30
- full enquiry interval 5-19
- function keys 7-11

G

- general help 7-14
- general help, System Manager 7-3
- generate default from this neighbor group, EGP 3-86
- generate default route, BGP 3-68
- generate default route, BGP configured neighbor 3-74
- generate default route, BGP group 3-71
- generate default route, EGP 3-83
- generate default routes from this neighbor, EGP 3-85
- getting started 1-3
 - on a PS/2 2-5
 - on a RISC System/6000 2-3
- group name, BGP 3-70
- group type, BGP 3-69

H

- hardware adapter parameters
 - Ethernet Adapter 5-6
 - Token-Ring Network 16/4 Adapter 5-3
 - X.25 adapter 5-30
- hardware requirements
 - description of configuration program 1-2
 - hardware and software requirements 2-5
 - installing the configuration program 2-5
 - starting the configuration program 2-6
 - using the Configuration Program 2-7
- Hardware Vital Product Data
 - description of 7-34

- Hardware Vital Product Data menu 7-34
- Hello

- broadcast 3-63
 - destination 3-65
 - destination mask 3-65
 - enable hello protocol 3-63
 - filter routes from 3-66
 - introduction 3-63
 - IP address of local interface 3-64, 3-66
 - IP address of remote router 3-66, 3-83
 - IP address of source router 3-64
 - IP address of trusted router 3-64
 - listen for Hello updates 3-64
 - name of import filter 3-65
 - preference 3-65
 - restrict routes 3-65
 - restrictions 3-63
 - route preference 3-63
 - send Hello updates 3-64
- hello interval, OSPF 3-54, 3-57
- Hello Protocol
 - broadcast 3-63
 - destination 3-65
 - destination mask 3-65
 - enable hello protocol 3-63
 - filter routes from 3-66
 - introduction 3-63
 - IP address of local interface 3-64, 3-66
 - IP address of remote router 3-66, 3-83
 - IP address of source router 3-64
 - IP address of trusted router 3-64
 - listen for Hello updates 3-64
 - name of import filter 3-65
 - preference 3-65
 - restrict routes 3-65
 - restrictions 3-63
 - route preference 3-63
 - send Hello updates 3-64
- hello time 3-5, 6-82
- hold time, BGP configured neighbor 3-76
- hold time, BGP group 3-72
- hop count, SRB port 6-27
- host address to filter on, IPX/RIP router 3-105
- host address to filter on, XNS 3-113
- host address, IPX/RIP router 3-105
- host address, XNS 3-113
- host name 10-34
- host name servers 10-37
- host name to IP address mapping 10-34
- host name, system management 4-21
- hosts that can perform configuration functions 4-18
- hour 4-20
- how to
 - Active Internet Connection Information 11-81
 - Bridge Statistics 11-74
 - Clean the Error Log 11-10
 - configuration program 2-2
 - Connection Statistics 11-70, 11-77

how to (*continued*)

- Copy Error Log or Trace Log to Transfer Directory 11-53
- Copy System Dump to Diskette or Transfer Directory 11-14
- Dump Adapter Memory 11-41
- Export Performance Data 11-89
- Export Problem Determination Output 11-53
- Extract Error Log Records From System Dump 11-15
- Extract Trace Log Records From System Dump 11-15
- Filter Information 11-73
- function keys 7-11
- LAN Bridge Internal Protocol Frame Statistics 11-86
- LAN Bridge Statistics 11-75, 11-85
- List Process Commands 11-62
- List Processes 11-61
- Main Window 2-7
- Memory Management Statistics 11-80
- Packet Traffic Statistics 11-72, 11-79
- Protocol Statistics 11-71
- Read Adapter Memory 11-38
- Set DECnet Trace Output 11-50
- Source Route Bridge Spanning Tree Frame Relay Statistics 11-82
- Source Route Bridge Spanning Tree Statistics 11-82
- Spanning Tree Statistics 11-82
- Start Adapter Line Trace 11-39
- Start and Stop SNMP Trace 11-28
- Start AppleTalk Protocol Trace 11-31
- Start APPN Trace 11-34
- Start APPN User Process Memory Dump 11-16
- Start Bridging Frame Trace 11-44
- Start IP Routing Protocols Dump 11-19
- Start IP Routing Protocols Trace 11-25
- Start System Dump 11-12
- Start System Trace 11-21
- Start User Process Memory Dump 11-16
- Stop AppleTalk Protocol Trace 11-32
- Stop APPN Trace 11-35
- Stop Bridging Frame Trace 11-45
- Stop IP Routing Protocols Trace 11-26
- Stop System Trace 11-22
- System Manager screens 7-3
- System Socket Information 11-81
- TCP/IP Protocol Statistics 11-77
- TCP/IP Route Statistics 11-80
- Transparent Bridge Spanning Tree Frame Relay Statistics 11-84
- Transparent Bridge Spanning Tree Statistics 11-83
- Use Adapter Debug Facility 11-37
- Use DECnet Debug Facility 11-48
- Use Source Route Bridging Debug Facility 11-42
- Use Special User Process Traces 11-24
- Use System and User Process Dump Facilities 11-11

how to (*continued*)

- Use System Trace Facility 11-21
- View a Formatted System Dump 11-14
- View Adapter Debug Data in Transfer Directory 11-41
- View Adapter Interface Statistics 11-69
- View Adapter Registers 11-39
- View an Error Report 11-6
- View an Error Report for a Single Sequence Number 11-8
- View AppleTalk Protocol Trace 11-32
- View APPN Trace Report 11-35
- View Bridge Configuration Information 11-46
- View Bridge SAP Filter Information 11-47
- View Bridge Trace Files 11-44
- View Bridging Frame Trace Output 11-45
- View DECnet Trace Output 11-52
- View Input/Output Statistics 11-88
- View IP Routing Protocols Dump 11-19
- View IP Routing Protocols Trace 11-26
- View Network Management Information 11-57
- View Previous System Dump Information 11-13
- View Process Information 11-63
- View Process Information and Status 11-61
- View Process Status 11-65
- View Process Table Information 11-67
- View Protocol and Interface Packet Traffic Information 11-55
- View Routing Data Structures 11-48
- View SNMP Trace 11-28
- View System Activity Report 11-59
- View System Monitor Trace 11-29
- View System Network Statistics 11-75
- View System Trace Report 11-22
- View User Process Memory Dump 11-17
- View Virtual Memory Statistics 11-87
- View X.25 Trace 11-30

I
IBM 6611

- publications xxvii
- IEEE 802.1D (transparent bridging) 3-10
- import default route, EGP 3-85, 3-87
- import name, BGP 3-78
- import route filters, BGP 3-78
- Import Software to Transfer Directory 12-7
- importing data 10-43
- inbound ring number filters 6-12
- inbound SNAP value filters 6-11
- include calling address in call request packets 5-40
- information message screens 7-3
- initial configuration 2-13
- installation and maintenance, software
 - automated software component installation for multiple IBM 6611s 12-23
 - automated software update installation for multiple IBM 6611s 12-21

installation and maintenance, software (*continued*)

- automated software update installation for one IBM 6611 12-19
- automating management of software changes 12-19
- Clean Up After a Failed Installation 12-16
- Commit Applied Updates (Delete Previous Version) 12-16
- description of 7-31
- exporting software vital product data 12-40
- Import Software to Transfer Directory 12-7
- installing software changes 12-3
- installing software components 12-5
- installing software updates 12-3
- List All Applied but Not Committed Software 12-16
- List All Installed Software 12-35
- List All Problems Fixed by Software Updates in Transfer Directory 12-8
- List All Software in the Transfer Directory 12-8
- List All Updates to a Software Component 12-35
- List Dependents of a Software Component 12-37
- List Files Included in a Software Component 12-36
- List Prerequisites of a Software Component 12-36
- post software installation functions 12-16
- Reinstate Saved Software Component 12-18
- Reject Applied Updates (Use Previous Version) 12-17
- Remove Saved Software Component 12-18
- Restart System After Applying New Software 12-13
 - restarting system after software installation 12-6
- saving software and configuration diskettes 12-33
- software component and update packaging 12-2
- software component installation procedure 12-12
- software installation procedure 12-6
- software update installation procedure 12-9
- software VPD 12-33
- transferring software changes 12-25
- transferring software changes, from IBM 6611 using FTP 12-30
- transferring software changes, from RISC System/6000 using FTP 12-28
- transferring software changes, from RISC System/6000 using Xmodem 12-32
- transferring software changes, IBM 6611 diskette 12-26
- transferring software changes, RISC System/6000 diskette 12-27
- Verify a Software Component 12-39
- View History of a Software Component 12-38
- View ID of a Software Component 12-38
- installing software 7-31
- installing software changes 12-3
- installing software components 12-5
- installing software updates 12-3
- interface IP address, BGP configured neighbor 3-74
- interface IP address, BGP group 3-71
- interface IP address, OSPF 3-52
- interface transit delay, OSPF 3-54
- interface transmit delay, OSPF 3-57
- interface type, OSPF 3-53, 3-55
- Internetwork Packet Exchange protocol
 - enable IPX router 3-102
 - filter ID 3-103, 3-105, 3-106, 3-108
 - filtering mode 3-103, 3-104, 3-106, 3-107
 - host address 3-105
 - host address to filter on 3-105
 - introduction 3-102
 - introduction SAP filters 3-102
 - local IPX network to filter on 3-108
 - local IPX networks to filter on 3-106
 - name 3-104
 - network 3-104
 - network number 3-103, 3-105, 3-107, 3-108
 - network numbers to filter on 3-105, 3-107, 3-108
 - server name 3-104
 - server type 3-103
 - split horizon for RIP filters 3-102
 - status of all defined inbound RIP filters 3-106
 - status of all defined outbound RIP filters 3-107
 - status of all defined RIP router filters 3-104
 - status of all defined SAP filters 3-102
 - type 3-103
- IP address 6-51, 10-34
- IP address of configuration hosts 4-18
- IP address of destination router, DECnet 3-27
- IP address of destination router, NetBIOS 3-47
- IP address of local interface, hello 3-64, 3-66
- IP address of local interface, RIP 3-59
- IP address of local interface, RIP imports 3-62
- IP address of name server 4-22
- IP address of neighbor router, OSPF 3-55
- IP address of remote host 4-21
- IP address of remote IBM 6611, data link switching 3-26
- IP address of remote router 3-66
- IP address of remote router, RIP imports 3-61
- IP address of remote time server 4-23
- IP address of source router, hello 3-64
- IP address of source router, RIP 3-59
- IP address of trusted router 3-60
- IP address of trusted router, hello 3-64
- IP address, BGP unconfigured neighbor 3-76
- IP address, SNMP 4-10
- IP filter ID, IP port filters 6-53
- IP network
 - 6611 Internet address 13-5
 - remote workstation for service 13-2, 13-5
- IP Packet Filter
 - filter ID 3-92
 - filter IP address 1 3-93
 - filter IP address 2 3-94
 - filter subnet mask 1 3-93
 - filter subnet mask 2 3-94
 - filter type 3-93
 - introduction 3-92

IP Packet Filter *(continued)*

- permit/deny traffic 3-93
- status of all defined IP filters 3-92

IP port filters 6-52

- IP port filters, filter IP address 1 6-54
- IP port filters, filter IP address 2 6-55
- IP port filters, filter subnet mask 1 6-55
- IP port filters, filter subnet mask 2 6-55
- IP port filters, filter type 6-54
- IP port filters, IP filter ID 6-53
- IP port filters, permit/deny traffic 6-54

IP routing protocols 3-51

- BGP 3-67
- EGP 3-83
- Hello 3-63
- OSPF 3-51
- RIP 3-58

IP Static Routes

- destination address 3-90
- destination mask 3-90, 3-114
- destination network number 3-114
- introduction 3-90
- next hop router 3-114
- next hop router 1 3-90
- next hop router 2 3-91
- next hop router 3 3-91
- preference 3-91
- restrictions 3-90
- retain route in master table 3-91

IPX

- enable IPX router 3-102
- filter ID 3-103, 3-105, 3-106, 3-108
- filtering mode 3-103, 3-104, 3-106, 3-107
- host address 3-105
- host address to filter on 3-105
- introduction 3-102
- introduction SAP filters 3-102
- local IPX network to filter on 3-108
- local IPX networks to filter on 3-106
- name 3-104
- network 3-104
- network number 3-103, 3-105, 3-107, 3-108
- network numbers to filter on 3-105, 3-107, 3-108
- server name 3-104
- server type 3-103
- split horizon for RIP filters 3-102
- status of all defined inbound RIP filters 3-106
- status of all defined outbound RIP filters 3-107
- status of all defined RIP router filters 3-104
- status of all defined SAP filters 3-102
- type 3-103

IPX network number 6-68

IPX port parameters 6-68

IPX SAP filters

- filter ID 3-103
- filtering mode 3-103
- introduction 3-102
- name 3-104

IPX SAP filters *(continued)*

- network 3-104
- network number 3-103
- server name 3-104
- server type 3-103
- status of all defined SAP filters 3-102
- type 3-103

L

LAN Bridging Protocol 5-12

- auto reboot on error 5-12
- enable configuration report saver 5-14
- enable LAN bridging protocol on this port 5-12
- enable ring error monitor 5-14
- enable ring parameter server 5-14
- event log drive 5-13
- introduction 5-12
- largest frame size 5-13
- link password 0 5-14
- link password 1 5-15
- link password 2 5-15
- link password 3 5-15
- memory dump on error 5-13
- performance counter threshold 5-12
- restrictions 5-12
- telecommunication link error threshold 5-12

largest frame size 5-13

level poll timer 5-46

link password 0 5-14

link password 1 5-15

link password 2 5-15

link password 3 5-15

link quality monitoring interval 5-17

List All Applied but Not Committed Software 12-16

List All Installed Software 12-35

List All Problems Fixed by Software Updates in Transfer Directory 12-8

List All Software in the Transfer Directory 12-8

List All Updates to a Software Component 12-35

List Dependents of a Software Component 12-37

List Files Included in a Software Component 12-36

List Prerequisites of a Software Component 12-36

listen for hello updates 3-64

listen for RIP updates 3-59

listing host name servers 10-37

listing host name to IP address mapping 10-36

listing time servers 10-40

listing userids and passwords 10-33

LMI option 5-19

local access configurations 9-2

local autonomous system number, BGP 3-68

local autonomous system number, EGP 3-83

local DECnet address 3-116

local DTE address (NUA) 5-33

local IPX network to filter on, IPX 3-106, 3-108

local XNS network to filter on 3-110, 3-111

- locally administered address, EIA 422/449 Serial Adapter 5-11
- locally administered address, Ethernet Adapter 5-7
- locally administered address, Token-Ring Network 16/4 Adapter 5-4
- lock value 4-5
- lock, software 10-57
- log, error
 - warning about erasing 11-5, 11-10
- logging in to an IBM 6611 9-23
- logging in to IBM 6611 9-23
 - userids and passwords 9-25
- logical channel (PVCs only) 5-47
- lowest LCN for 2-way SVCs 5-34
- lowest LCN for incoming SVCs 5-34
- lowest LCN for outgoing SVCs 5-33
- lowest LCN for PVCs 5-35

M

- MAC address format, token-ring 5-4
- MAC address, Ethernet Adapter 5-6
- MAC address, Token-Ring Network 16/4 Adapter 5-3
- maintenance
 - automated software component installation for multiple IBM 6611s 12-23
 - automated software update installation for multiple IBM 6611s 12-21
 - automated software update installation for one IBM 6611 12-19
 - automating management of software changes 12-19
 - Clean Up After a Failed Installation 12-16
 - Commit Applied Updates (Delete Previous Version) 12-16
 - description of 7-31
 - exporting software vital product data 12-40
 - Import Software to Transfer Directory 12-7
 - installing software changes 12-3
 - installing software components 12-5
 - installing software updates 12-3
 - List All Applied but Not Committed Software 12-16
 - List All Installed Software 12-35
 - List All Problems Fixed by Software Updates in Transfer Directory 12-8
 - List All Software in the Transfer Directory 12-8
 - List All Updates to a Software Component 12-35
 - List Dependents of a Software Component 12-37
 - List Files Included in a Software Component 12-36
 - List Prerequisites of a Software Component 12-36
 - post software installation functions 12-16
 - Reinstate Saved Software Component 12-18
 - Reject Applied Updates (Use Previous Version) 12-17
 - Remove Saved Software Component 12-18
 - Restart System After Applying New Software 12-13
 - restarting system after software installation 12-6
 - saving software and configuration diskettes 12-33

maintenance (*continued*)

- software component and update packaging 12-2
- software component installation procedure 12-12
- software installation procedure 12-6
- software update installation procedure 12-9
- software VPD 12-33
- transferring software changes 12-25
- transferring software changes, from IBM 6611 using FTP 12-30
- transferring software changes, from RISC System/6000 using FTP 12-28
- transferring software changes, from RISC System/6000 using Xmodem 12-32
- transferring software changes, IBM 6611 diskette 12-26
- transferring software changes, RISC System/6000 diskette 12-27
- Verify a Software Component 12-39
- View History of a Software Component 12-38
- View ID of a Software Component 12-38
- management, system
 - Adapter and Protocol Configuration 7-36
 - Concurrent Hardware Diagnostics 7-25
 - Configuration Files and Reports 7-35
 - flowchart 7-17
 - Hardware Vital Product Data 7-34
 - menu screens 7-17
 - Performance and Statistics 7-22
 - performing 7-16
 - Problem Determination Facilities 7-23
 - Remote Accesses to Other Nodes 7-30
 - Resource Control and Management 7-27
 - Software Installation and Maintenance 7-31
 - System Environment and Configuration 7-28
- managing ARP tables 10-13
- mask, BGP unconfigured neighbor 3-77
- maximum active neighbors, EGP 3-84
- maximum address 3-118
- maximum age 3-5
- maximum area 3-118
- maximum broadcast non-routers 3-119
- maximum broadcast routers 3-118
- maximum cost 3-117
- maximum hops 3-117
- maximum I-field size 5-28
- maximum initial packet size, EGP 3-83
- maximum number of clear packets 5-45
- maximum number of reset packets 5-45
- maximum receive unit 5-16
- maximum routers 6-83
- maximum transmission unit 6-5, 6-52
- maximum visits 3-118
- memory dump on error 5-13
- menu for
 - Performance and Statistics 11-55
 - Problem Determination Facilities 11-4
 - Use Adapter Debug Facility 11-37
 - Use DECnet Debug Facility 11-48

menu for *(continued)*

- Use Source Route Bridging Debug Facility 11-43
- Use Special User Process Traces 11-24
- Use System and User Process Dump Facilities 11-11
- Use System Trace Facility 11-21
- View Adapter Interface Statistics 11-69
- View an Error Report 11-7
- View Process Information and Status 11-61
- View System Network Statistics 11-76

menu screens 7-4

menus, Diagnostic Programs

- Diagnostic Mode Selection 13-2
 - error log analysis 13-2
 - Problem Determination option 13-2
 - System Verification option 13-2
- Diagnostic Operating Instructions 13-2
- Function Selection 13-2
 - device list 13-2
 - Diagnostic Routines 13-2
- Hardware Diagnostics 13-2
- System Manager 13-2

metric out, BGP configured neighbor 3-73

metric out, BGP group 3-70

metric, exports 3-96

MIB subtree 4-13

MIBs

- enable coldStart trap 4-10
- enable egpNeighborLoss trap 4-12
- enable enterpriseSpecific trap 4-12
- enable linkDown trap 4-11
- enable linkUp trap 4-11
- enable warmStart trap 4-10
- enterprise-specific trap throttle time 4-8

Microsoft Windows

- Configuration Program 2-6

minimum hello interval, EGP 3-85, 3-87

minimum polling interval, EGP 3-85, 3-87

minute 4-20

modem

- attached ASCII terminal 13-5

modem connection 9-17

modes, Diagnostic Program

- concurrent 13-2, 13-5

month 4-19

multicast MAC address 5-8

Multiprotocol Network Program

- publications xxvii

N

N2 counter 5-45

name of import filter 3-60

name of import filter, hello 3-65

name servers 4-22, 10-37

name, IPX 3-104

neighbor ASN, EGP 3-84

neighbor IP address, EGP 3-84

neighbor name, BGP unconfigured neighbor 3-77

NetBIOS

- destination name 3-47, 3-49, 3-50
- destination name filter type 3-49
- introduction 3-47
- IP address of destination router 3-47
- source name 3-48, 3-49
- source name filter type 3-48
- status of all defined NetBIOS destination name filters 3-49
- status of all defined NetBIOS source name filters 3-48

network

IP 13-2

- remote workstation for service 13-2, 13-5

network access to other nodes

- a local IBM 6611 9-6
- a remote IBM 6611 9-7
- controlling user tasks 9-25
- direct IP attachment 14-12
- direct-attached terminal 9-3
- extended network configurations 9-6
- FTP transfer method 14-14
- IP network connection 9-7
- local access configurations 9-2
- logging in to an IBM 6611 9-23
- modem 9-17
- modem transfer method 14-12
- modem-attached terminal 9-5
- network-attached terminal 9-4
- remote access configurations 9-4
- standalone IBM 6611 9-2
- through an EIA 232 serial port 9-19
- userid and passwords 9-25
- using the FTP 10-52
- using Xmodem 10-55
- viewing user tasks 9-25

network identifier 5-33

network management parameters

- address mask 4-18
- apply configuration 4-19
- baud rate for S1 serial port 4-4
- baud rate for S2 serial port 4-4
- community access 4-15
- community address 4-14
- community address mask 4-14
- community name 4-14
- community view name 4-15
- configuration hosts 4-18
- controlling password 4-16
- controlling userid 4-16
- day 4-19
- description of 4-2
- domain name 4-3
- EIA serial ports 4-4
- enable coldStart trap 4-10
- enable egpNeighborLoss trap 4-12

network management parameters (*continued*)

- enable enterpriseSpecific trap 4-12
- enable linkDown trap 4-11
- enable linkUp trap 4-11
- enable name resolution by remote name servers 4-22
- enable time service by remote time servers 4-23
- enable warmStart trap 4-10
- enterprise-specific trap throttle time 4-8
- host name 4-3, 4-21
- hosts that can perform configuration functions 4-18
- hour 4-20
- IP address 4-18
- IP address of host 4-21
- IP address of name server 4-22
- IP address of remote time server 4-23
- lock/unlocking the Multiprotocol Network Program 4-5
- MIB subtree 4-13
- minute 4-20
- month 4-19
- remote host names 4-21
- router serial number prefix 4-8
- router serial number suffix 4-9
- SNMP 4-6
- system contact 4-7
- system location 4-7
- system name 4-7
- time to perform configuration 4-19
- trap address 4-10
- trap community name 4-10
- userids and passwords 4-16
- view name 4-12
- viewing password 4-17
- viewing userid 4-16
- year 4-19
- network mask, OSPF 3-55
- network number, IPX 3-103, 3-107, 3-108
- network number, IPX port 6-68
- network number, IPX/RIP router 3-105
- network number, OSPF 3-55
- network number, XNS 3-110, 3-112, 3-113, 6-75
- network numbers to filter on, IPX 3-107, 3-108
- network numbers to filter on, IPX/RIP router 3-105
- network numbers to filter on, XNS 3-110, 3-112, 3-113
- next hop address of domain name 3-87
- next hop destination, BGP configured neighbor 3-73
- next hop destination, BGP group 3-70
- next hop router 1, IP static routes 3-90
- next hop router 2, IP static routes 3-91
- next hop router 3, IP static routes 3-91
- next hop router host address, XNS static routes 3-114
- next hop router, XNS static routes 3-114
- node type 3-116
- notice, warning
 - about erasing error log 11-5, 11-10
 - System Manager Configuration 7-36

- number of bytes returned in an error protocol packet 6-76
- number of LCNs for 2-way SVCs 5-34
- number of LCNs for outgoing SVCs 5-33
- number of LCNs for PVCs 5-35
- number of logical channels for incoming SVCs 5-35
- number, IPX 3-104

O

Open Shortest Path First

- area ID 3-51
- area type 3-52
- authentication type 3-52
- authorization key 3-53, 3-56
- cost 3-53
- eligible to become a designated router 3-55
- enable OSPF 3-51
- Hello interval 3-54, 3-57
- interface IP address 3-52
- interface transit delay 3-54
- interface transmit delay 3-57
- interface type 3-55
- IP address of neighbor router 3-55
- network mask 3-55
- network number 3-55
- poll interval 3-53
- retransmit interval 3-54, 3-56
- router dead interval 3-54, 3-57
- router ID 3-51
- router priority 3-53
- stub cost 3-52
- transit area ID 3-56
- virtual link ID 3-56
- virtual neighbor ID 3-56

operating

- configuration program 2-2
- IBM 6611 10-1
- resource control and management 10-1
- System Manager 7-2
- System Manager tasks 10-1

OSPF

- area ID 3-51
- area type 3-52
- authentication type 3-52
- authorization key 3-53, 3-56
- cost 3-53
- eligible to become a designated router 3-55
- enable OSPF 3-51
- Hello interval 3-54, 3-57
- interface IP address 3-52
- interface transit delay 3-54
- interface transmit delay 3-57
- interface type 3-55
- IP address of neighbor router 3-55
- network mask 3-55
- network number 3-55
- poll interval 3-53

OSPF (continued)

- retransmit interval 3-54, 3-56
- router dead interval 3-54, 3-57
- router ID 3-51
- router priority 3-53
- stub cost 3-52
- transit area ID 3-56
- virtual link ID 3-56
- virtual neighbor ID 3-56

P

- packet size and packet window size negotiation 5-42
- packet size negotiation facility 5-41
- packet type value, IPX port 6-70
- packet type value, XNS 6-78
- packet window size negotiation facility 5-42
- passive, BGP configured neighbor 3-75
- passive, BGP group 3-71
- passwords 9-8, 9-10, 9-13, 9-25
- passwords and userids 10-31
- path cost 6-6
- Performance and Statistics
 - Active Internet Connection Information 11-81
 - Bridge Statistics 11-74
 - Connection Statistics 11-70, 11-77
 - description of 7-22
 - Export Performance Data 11-89
 - Filter Information 11-73
 - LAN Bridge Internal Protocol Frame Statistics 11-86
 - LAN Bridge Statistics 11-75, 11-85
 - List Process Commands 11-62
 - List Processes 11-61
 - Memory Management Statistics 11-80
 - Packet Traffic Statistics 11-72, 11-79
 - Protocol Statistics 11-71
 - selecting a 11-54
 - Source Route Bridge Spanning Tree Frame Relay Statistics 11-82
 - Source Route Bridge Spanning Tree Statistics 11-82
 - Spanning Tree Statistics 11-82
 - System Socket Information 11-81
 - TCP/IP Protocol Statistics 11-77
 - TCP/IP Route Statistics 11-80
 - Transparent Bridge Spanning Tree Frame Relay Statistics 11-84
 - Transparent Bridge Spanning Tree Statistics 11-83
 - View Adapter Interface Statistics 11-69
 - View Input/Output Statistics 11-88
 - View Network Management Information 11-57
 - View Process Information 11-63
 - View Process Information and Status 11-61
 - View Process Status 11-65
 - View Process Table Information 11-67
 - View Protocol and Interface Packet Traffic Information 11-55

Performance and Statistics (continued)

- View System Activity Report 11-59
- View System Network Statistics 11-75
- View Virtual Memory Statistics 11-87
- Performance and Statistics menu 7-22
- performance and statistics tasks
- performance counter threshold 5-12
- permit/deny traffic 3-93
- permit/deny traffic, DECnet 3-120
- permit/deny traffic, IP port filters 6-54
- Personal System/2 or equivalent
 - description of configuration program 1-2
 - hardware and software requirements 2-5
 - installing the configuration program 2-5
 - starting the configuration program 2-6
 - using the Configuration Program 2-7
- physical link type 5-22
- physical link types
 - EIA 232-D 5-22
 - V.35 5-22
 - X.21 5-22
- ping 9-7
- point-to-point protocol 5-16
- Point-to-Point Protocol (PPP) parameters
 - enable link quality monitoring 5-16
 - introduction 5-16
 - link quality monitoring interval 5-17
 - maximum receive unit 5-16
 - restriction 5-16
- poll interval, OSPF 3-53
- polling interval 5-19
- pop-up lists 7-3
- port-level parameters
 - AppleTalk 6-57
 - DECnet 6-82
 - description of 6-3
 - Internet Protocol (IP) 6-51
 - Internetwork Packet Exchange (IPX) 6-68
 - NetBIOS 6-50
 - source route bridging 6-5
 - source route bridging filters 6-8
 - Systems Network Architecture (SNA) 6-49
 - transparent bridging 6-29
 - transparent bridging filters 6-32
 - Xerox Network Systems (XNS) 6-75
- post software installation functions 12-16
- preference, BGP configured neighbor 3-75
- preference, BGP group 3-72
- preference, BGP import destination 3-82
- preference, BGP import filters 3-81
- preference, EGP 3-83, 3-86
- preference, EGP imports 3-88, 3-89
- preference, hello 3-65
- preference, IP static routes 3-91
- preference, RIP imports 3-61
- preparing for configuration
 - system configuration A-2

- primary repoll count 5-28
- primary repoll threshold 5-27
- primary repoll timeout 5-29
- primary slow list timeout 5-27
- Problem Determination Facilities
 - description of 7-23
 - using the performance and statistics facilities 11-54
 - using the System Manager 11-3
- Problem Determination Facilities menu 7-23
- problem determination tasks
 - Clean the Error Log 11-10
 - Copy Error Log or Trace Log to Transfer Directory 11-53
 - Copy System Dump to Diskette or Transfer Directory 11-14
 - Dump Adapter Memory 11-41
 - Export Problem Determination Output 11-53
 - Extract Error Log Records From System Dump 11-15
 - Extract Trace Log Records From System Dump 11-15
 - Read Adapter Memory 11-38
 - selecting a 11-3
 - Set DECnet Trace Output 11-50
 - Start Adapter Line Trace 11-39
 - Start and Stop SNMP Trace 11-28
 - Start AppleTalk Protocol Trace 11-31
 - Start APPN Trace 11-34
 - Start APPN User Process Memory Dump 11-16
 - Start Bridging Frame Trace 11-44
 - Start IP Routing Protocols Dump 11-19
 - Start IP Routing Protocols Trace 11-25
 - Start System Dump 11-12
 - Start System Trace 11-21
 - Start User Process Memory Dump 11-16
 - Stop AppleTalk Protocol Trace 11-32
 - Stop APPN Trace 11-35
 - Stop Bridging Frame Trace 11-45
 - Stop IP Routing Protocols Trace 11-26
 - Stop System Trace 11-22
 - Use Adapter Debug Facility 11-37
 - Use DECnet Debug Facility 11-48
 - Use Source Route Bridging Debug Facility 11-42
 - Use Special User Process Traces 11-24
 - Use System and User Process Dump Facilities 11-11
 - Use System Trace Facility 11-21
 - View a Formatted System Dump 11-14
 - View Adapter Debug Data in Transfer Directory 11-41
 - View Adapter Registers 11-39
 - View an Error Report 11-6
 - View an Error Report for a Single Sequence Number 11-8
 - View AppleTalk Protocol Trace 11-32
 - View APPN Trace Report 11-35
 - View Bridge Configuration Information 11-46

- problem determination tasks (*continued*)
 - View Bridge SAP Filter Information 11-47
 - View Bridge Trace Files 11-44
 - View Bridging Frame Trace Output 11-45
 - View DECnet Trace Output 11-52
 - View IP Routing Protocols Dump 11-19
 - View IP Routing Protocols Trace 11-26
 - View Previous System Dump Information 11-13
 - View Routing Data Structures 11-48
 - View SNMP Trace 11-28
 - View System Monitor Trace 11-29
 - View System Trace Report 11-22
 - View User Process Memory Dump 11-17
 - View X.25 Trace 11-30
- protocol configuration parameters
 - AppleTalk 6-57
 - DECnet 6-82
 - description of 6-3
 - Internet Protocol (IP) 6-51
 - Internetwork Packet Exchange (IPX) 6-68
 - NetBIOS 6-50
 - source route bridging 6-5
 - source route bridging filters 6-8
 - Systems Network Architecture (SNA) 6-49
 - transparent bridging 6-29
 - transparent bridging filters 6-32
 - Xerox Network Systems (XNS) 6-75
- protocol-dependent parameters
 - BGP 3-67
 - data link switching 3-18
 - DECnet 3-115
 - EGP 3-83
 - export filters 3-95
 - Hello 3-63
 - IP over X.25 3-100
 - NetBIOS 3-47
 - OSPF 3-51
 - packet filters 3-92
 - RIP 3-58
 - source route bridging 3-4
 - starting 3-3
 - Static Routes 3-90
 - transparent bridging 3-10
 - XNS 3-109
- protocol-independent parameters
 - address mask 4-18
 - apply configuration 4-19
 - baud rate for S1 serial port 4-4
 - baud rate for S2 serial port 4-4
 - community access 4-15
 - community address 4-14
 - community address mask 4-14
 - community name 4-14
 - community view name 4-15
 - configuration hosts 4-18
 - controlling password 4-16
 - controlling userid 4-16
 - day 4-19

protocol-independent parameters (*continued*)

- description of 4-2
- domain name 4-3
- EIA serial ports 4-4
- enable coldStart trap 4-10
- enable egpNeighborLoss trap 4-12
- enable enterpriseSpecific trap 4-12
- enable linkDown trap 4-11
- enable linkUp trap 4-11
- enable name resolution by remote name servers 4-22
- enable time service by remote time servers 4-23
- enable warmStart trap 4-10
- enterprise-specific trap throttle time 4-8
- host name 4-3, 4-21
- hosts that can perform configuration functions 4-18
- hour 4-20
- IP address 4-18
- IP address of host 4-21
- IP address of name server 4-22
- IP address of remote time server 4-23
- lock/unlocking the Multiprotocol Network Program 4-5
- MIB subtree 4-13
- minute 4-20
- month 4-19
- remote host names 4-21
- router serial number prefix 4-8
- router serial number suffix 4-9
- SNMP 4-6
- system contact 4-7
- system location 4-7
- system name 4-7
- time to perform configuration 4-19
- trap address 4-10
- trap community name 4-10
- userids and passwords 4-16
- view name 4-12
- viewing password 4-17
- viewing userid 4-16
- year 4-19
- protocols 6-4
 - encapsulation 6-4
- PTFs 12-2
- publications
 - IBM 6611 xxvii
- PVC auto-reset value 5-38
- PVC logical channel number 5-37
- PVC receive packet size 5-37, 5-38
- PVC receive packet window size 5-38, 5-39
- PVC transmit packet size 5-38, 5-39
- PVC transmit packet window size 5-38, 5-39

R

- receive packet size, SVC 5-48
- receive packet window size, PVC 5-39

- receive packet window size, SVC 5-48
- Reinstate Saved Software Component 12-18
- Reject Applied Updates (Use Previous Version) 12-17
- rejecting configuration changes to configuration database 10-42
- relational compare operator, IPX port 6-71
- relational compare operator, XNS 6-79
- remote access configurations 9-4
- Remote Accesses to Other Nodes
 - description of 7-30
- Remote Accesses to Other Nodes menu 7-30
- remote DECnet address 6-82, 6-84
- remote DECnet node type 6-82, 6-84
- remote DTE address (SVCs only) 5-47
- remote execution 9-7, 9-13, 9-15
- Remote Execution Protocol
 - 3-digit display command primitive 8-100
 - accessing 8-7
 - adapter debug facility command primitives 8-10
 - address resolution protocol: adapter command primitives 8-12
 - address resolution protocol: system command primitives 8-16
 - bridging debug facility command primitives 8-19
 - configuration command primitives 8-25
 - DECnet debug facility command primitives 8-29
 - diskette command primitives 8-37
 - dump: system command primitives 8-40
 - dump: user process command primitives 8-42
 - entering 7-16
 - error report command primitives 8-43
 - executing the command primitives 8-6
 - fast-path exit command primitives 8-53
 - file management command primitives 8-54
 - getting help 8-8
 - hardware VPD command primitives 8-57
 - host name command primitives 8-60
 - host name to IP address mapping command primitives 8-61
 - install command primitives 8-62
 - name server command primitives 8-66
 - process command primitives 8-68
 - remote access command primitives 8-70
 - returning 7-16
 - route table command primitives 8-73
 - serial port command primitives 8-74
 - shutdown: system command primitives 8-76
 - software lock command primitive 8-78
 - software VPD command primitives 8-79
 - statistic-gathering command primitives 8-81
 - terminal control primitives 8-86
 - time server command primitives 8-87
 - time: system command primitives 8-89
 - trace: system command primitives 8-91
 - trace: user process command primitives 8-94
 - user: system command primitives 8-98
- remote host names 4-21

- remote login 9-10, 9-12
- remote shell 9-7, 9-14, 9-15
- Remote Shell Protocol
 - 3-digit display command primitive 8-100
 - accessing 8-7
 - adapter debug facility command primitives 8-10
 - address resolution protocol: adapter command primitives 8-12
 - address resolution protocol: system command primitives 8-16
 - bridging debug facility command primitives 8-19
 - configuration command primitives 8-25
 - DECnet debug facility command primitives 8-29
 - diskette command primitives 8-37
 - dump: system command primitives 8-40
 - dump: user process command primitives 8-42
 - entering 7-16
 - error report command primitives 8-43
 - executing the command primitives 8-6
 - fast-path exit command primitives 8-53
 - file management command primitives 8-54
 - getting help 8-8
 - hardware VPD command primitives 8-57
 - host name command primitives 8-60
 - host name to IP address mapping command primitives 8-61
 - install command primitives 8-62
 - name server command primitives 8-66
 - process command primitives 8-68
 - remote access command primitives 8-70
 - returning 7-16
 - route table command primitives 8-73
 - serial port command primitives 8-74
 - shutdown: system command primitives 8-76
 - software lock command primitive 8-78
 - software VPD command primitives 8-79
 - statistic-gathering command primitives 8-81
 - terminal control primitives 8-86
 - time server command primitives 8-87
 - time: system command primitives 8-89
 - trace: system command primitives 8-91
 - trace: user process command primitives 8-94
 - user: system command primitives 8-98
- Remove Saved Software Component 12-18
- request to send 5-23
- Resource Control and Management
 - adding adapter ARP table entries 10-15
 - adding system ARP table entries 10-14
 - clearing adapter ARP table 10-17
 - deleting adapter ARP table entries with hardware address 10-16
 - deleting adapter ARP table entries with host name 10-17
 - deleting system ARP table entries 10-15
 - description of 7-27
 - exporting the route table information 10-18
 - managing ARP tables 10-13
 - reading the three-digit display 10-6

- Resource Control and Management (*continued*)
 - shutting down the IBM 6611 10-4
 - starting the IBM 6611 10-4
 - stopping the IBM 6611 10-4
 - using the menu items 10-3
 - viewing adapter AARP table entries 10-17
 - viewing adapter ARP table entries 10-15
 - viewing system ARP table entries 10-14
 - viewing the adapter route tables 10-9
 - viewing the network management subsystem information 10-11
 - viewing the system routing table 10-7
- Resource Control and Management menu 7-27
- Restart System After Applying New Software 12-13
- restarting system after software installation 12-6
- restarting the IBM 6611 10-4
- restrict imports, BGP import filters 3-81
- restrict routes, BGP import destination 3-82
- restrict routes, EGP imports 3-89
- restrict routes, hello 3-65
- restrict, EGP imports 3-88
- restrict, exports 3-96
- restrict, RIP imports 3-61
- retain route in master table, IP static routes 3-91
- retransmit count 5-27
- retransmit interval, OSPF 3-54, 3-56
- reverse charging/fast select facility 5-42
- REXEC 9-13, 9-15
 - 3-digit display command primitive 8-100
 - accessing 8-7
 - adapter debug facility command primitives 8-10
 - address resolution protocol: adapter command primitives 8-12
 - address resolution protocol: system command primitives 8-16
 - bridging debug facility command primitives 8-19
 - configuration command primitives 8-25
 - DECnet debug facility command primitives 8-29
 - diskette command primitives 8-37
 - dump: system command primitives 8-40
 - dump: user process command primitives 8-42
 - entering 7-16
 - error report command primitives 8-43
 - executing the command primitives 8-6
 - fast-path exit command primitives 8-53
 - file management command primitives 8-54
 - getting help 8-8
 - hardware VPD command primitives 8-57
 - host name command primitives 8-60
 - host name to IP address mapping command primitives 8-61
 - install command primitives 8-62
 - name server command primitives 8-66
 - process command primitives 8-68
 - remote access command primitives 8-70
 - returning 7-16
 - route table command primitives 8-73
 - serial port command primitives 8-74

REXEC (continued)

- shutdown: system command primitives 8-76
- software lock command primitive 8-78
- software VPD command primitives 8-79
- statistic-gathering command primitives 8-81
- terminal control primitives 8-86
- time server command primitives 8-87
- time: system command primitives 8-89
- trace: system command primitives 8-91
- trace: user process command primitives 8-94
- user: system command primitives 8-98

ring number 6-5

ring number for inbound ring number filters 6-13

ring number mask for inbound ring number filters 6-13

ring number mask, SRB port 6-23

ring number, SRB port 6-23

ring numbers to DLCI numbers 6-5

RIP 3-58

- broadcast 3-58
- destination 3-60
- destination mask 3-60
- enable RIP 3-58
- filter routes from 3-61
- introduction 3-58
- IP address of local interface 3-59, 3-62
- IP address of remote router 3-61
- IP address of source router 3-59
- IP address of trusted router 3-60
- listen for RIP updates 3-59
- name of import filter 3-60
- preference 3-61
- restrict 3-61
- restrictions 3-58
- route preference 3-59
- send RIP updates 3-60
- zero reserved fields 3-58

RISC System/6000

- as a network management station 12-19
- description of configuration program 1-2
- installing the configuration program 2-3
- starting the configuration program 2-4
- transferring software changes 12-27, 12-28
- using the configuration program 2-3, 2-7

rlogin 9-7, 9-10, 9-12

route preference, hello 3-63

route preference, RIP 3-59

route tables, exporting 10-18

router dead interval, OSPF 3-54, 3-57

router ID 3-51

router priority 6-83

router priority, OSPF 3-53

router serial number prefix 4-8

router serial number suffix 4-9

router-to-router protocols

- BGP 3-67
- EGP 3-83
- Hello 3-63

router-to-router protocols (continued)

- OSPF 3-51
- RIP 3-58

routing buffer size 3-119

Routing Information Protocol

- broadcast 3-58
- destination 3-60
- destination mask 3-60
- enable RIP 3-58
- filter routes from 3-61
- introduction 3-58
- IP address of local interface 3-59, 3-62
- IP address of remote router 3-61
- IP address of source router 3-59
- IP address of trusted router 3-60
- listen for RIP updates 3-59
- name of import filter 3-60
- preference 3-61
- restrict 3-61
- restrictions 3-58
- route preference 3-59
- send RIP updates 3-60
- zero reserved fields 3-58

routing timer 6-83

RPOA indices 5-49

RSH 9-14, 9-15

- 3-digit display command primitive 8-100
- accessing 8-7
- adapter debug facility command primitives 8-10
- address resolution protocol: adapter command primitives 8-12
- address resolution protocol: system command primitives 8-16
- bridging debug facility command primitives 8-19
- configuration command primitives 8-25
- DECnet debug facility command primitives 8-29
- diskette command primitives 8-37
- dump: system command primitives 8-40
- dump: user process command primitives 8-42
- entering 7-16
- error report command primitives 8-43
- executing the command primitives 8-6
- fast-path exit command primitives 8-53
- file management command primitives 8-54
- getting help 8-8
- hardware VPD command primitives 8-57
- host name command primitives 8-60
- host name to IP address mapping command primitives 8-61
- install command primitives 8-62
- name server command primitives 8-66
- process command primitives 8-68
- remote access command primitives 8-70
- returning 7-16
- route table command primitives 8-73
- serial port command primitives 8-74
- shutdown: system command primitives 8-76
- software lock command primitive 8-78

RSH (*continued*)

- software VPD command primitives 8-79
- statistic-gathering command primitives 8-81
- terminal control primitives 8-86
- time server command primitives 8-87
- time: system command primitives 8-89
- trace: system command primitives 8-91
- trace: user process command primitives 8-94
- user: system command primitives 8-98

S

SAP value 6-49

scrolling 7-11

SDLC Adapter 5-21

- data rate select 5-23
- data terminal ready 5-24
- enable interface 5-22
- introduction 5-21
- physical link type 5-22
- request to send 5-23
- restrictions 5-22
- serial encoding 5-23

selector screens 7-6

selling to a third party 10-57

send hello updates 3-64

send RIP updates 3-60

sending an AT command 10-22

Serial Adapter parameters

- compatible protocols 5-9
- cylink serial number 5-10
- data encoding 5-11
- data link protocols 5-9
- enable interface 5-10
- introduction 5-9
- locally administered MAC address 5-11
- serial line speed 5-10

serial encoding 5-23

serial line speed 5-10

serial port access 9-19

S1 port access 9-19

S2 port access 9-19

serial port, S1 4-4

serial port, S2 4-4

serial ports

ASCII terminal connection 13-2, 13-5

serial ports (EIA), configuring 4-4

server name, IPX 3-104

server type, IPX 3-103

service, 6611

ASCII terminal 13-2, 13-5

remote IP workstation 13-2, 13-5

setting passwords 9-8, 9-10, 9-13

setting the host name and domain name 10-35

setting userids 9-8, 9-10, 9-13

shutting down the IBM 6611 10-4

Simple Network Management Protocol

community access 4-15

Simple Network Management Protocol (*continued*)

- community address 4-14
- community address mask 4-14
- community name 4-14
- community view name 4-15
- enable coldStart trap 4-10
- enable egpNeighborLoss trap 4-12
- enable enterpriseSpecific trap 4-12
- enable linkDown trap 4-11
- enable linkUp trap 4-11
- enable SNMP 4-6
- enable warmStart trap 4-10
- enterprise-specific trap throttle time 4-8
- explanation on communities 4-13
- introduction 4-6
- MIB subtree 4-13
- restrictions 4-6
- router serial number prefix 4-8
- router serial number suffix 4-9
- rules for object identifiers and names 4-6
- system contact 4-7
- system location 4-7
- system name 4-7
- trap address 4-10
- trap community name 4-10
- view name 4-12

SM Configuration Facility

- configuration error message report 14-22
- configuration objects 14-7
- configuration procedure 14-8
- configuration script 14-23
- description of 1-2, 7-36
- direct IP attachment 14-12
- FTP transfer method 14-14
- importing and exporting the configuration file 14-17
- initial configuration using a diskette 14-11
- initial configuration without a diskette 14-11
- minimal configuration using System Manager 14-15
- modem transfer method 14-12
- port-level list object 14-43
- port-level single objects 14-34
- reinstating a saved configuration file 14-19
- system-level list object 14-50
- system-level single objects 14-26
- updating configuration parameters 14-4
- using configuration information text files 14-20

SNA

- destination address 3-29, 3-31
- destination address mask 3-29, 3-31
- destination frame filter type 3-30
- filter ID 3-28, 3-30
- IP address of destination router 3-27
- source address 3-28, 3-30
- source address mask 3-29, 3-30
- source frame filter type 3-28
- status of all defined SNA destination frame filters 3-29

SNA (continued)

status of all defined SNA source frame filters 3-27

SNA stations 5-25

- force disconnect timeout 5-29
- introduction 5-25
- maximum l-field size 5-28
- primary repoll count 5-28
- primary repoll threshold 5-27
- primary repoll timeout 5-29
- primary slow list timeout 5-27
- restrictions 5-25
- retransmit count 5-27
- retransmit threshold 5-27
- station address 5-25
- station token-ring destination address 5-26
- station token-ring destination SAP 5-26
- station token-ring source address 5-25
- station token-ring source SAP 5-25
- transmit window count 5-28

SNAP value 6-21

SNAP value mask on SRB port 6-12

SNAP value on SRB port 6-12

SNMP parameters

- community access 4-15
- community address 4-14
- community address mask 4-14
- community name 4-14
- community view name 4-15
- enable coldStart trap 4-10
- enable egpNeighborLoss trap 4-12
- enable enterpriseSpecific trap 4-12
- enable linkDown trap 4-11
- enable linkUp trap 4-11
- enable SNMP 4-6
- enable warmStart trap 4-10
- enterprise-specific trap throttle time 4-8
- explanation on communities 4-13
- introduction 4-6
- MIB subtree 4-13
- restrictions 4-6
- router serial number prefix 4-8
- router serial number suffix 4-9
- rules for object identifiers and names 4-6
- system contact 4-7
- system location 4-7
- system name 4-7
- trap address 4-10
- trap community name 4-10
- view name 4-12

SNMP traps

- enable coldStart trap 4-10
- enable egpNeighborLoss trap 4-12
- enable enterpriseSpecific trap 4-12
- enable linkDown trap 4-11
- enable linkUp trap 4-11
- enable warmStart trap 4-10
- enterprise-specific trap throttle time 4-8

software changes, transferring 12-25

software changes, transferring from IBM 6611 using FTP 12-30

software changes, transferring from RISC System/6000 using \TP 12-28

software changes, transferring from RISC System/6000 using Xmodem 12-32

software changes, transferring to IBM 6611 diskette 12-26

software changes, transferring to RISC System/6000 diskette 12-27

software component installation procedure 12-12

software components 12-2

software diskettes 12-33

Software Installation and Maintenance

automated software component installation for multiple IBM 6611s 12-23

automated software update installation for multiple IBM 6611s 12-21

automated software update installation for one IBM 6611 12-19

automating management of software

changes 12-19

Clean Up After a Failed Installation 12-16

Commit Applied Updates (Delete Previous Version) 12-16

description of 7-31

exporting software vital product data 12-40

Import Software to Transfer Directory 12-7

installing software changes 12-3

installing software components 12-5

installing software updates 12-3

List All Applied but Not Committed Software 12-16

List All Installed Software 12-35

List All Problems Fixed by Software Updates in Transfer Directory 12-8

List All Software in the Transfer Directory 12-8

List All Updates to a Software Component 12-35

List Dependents of a Software Component 12-37

List Files Included in a Software Component 12-36

List Prerequisites of a Software Component 12-36

post software installation functions 12-16

Reinstate Saved Software Component 12-18

Reject Applied Updates (Use Previous Version) 12-17

Remove Saved Software Component 12-18

Restart System After Applying New Software 12-13

restarting system after software installation 12-6

saving software and configuration diskettes 12-33

software component and update packaging 12-2

software component installation procedure 12-12

software installation procedure 12-6

software update installation procedure 12-9

software VPD 12-33

transferring software changes 12-25

transferring software changes, from IBM 6611 using FTP 12-30

transferring software changes, from RISC System/6000 using FTP 12-28

Software Installation and Maintenance (*continued*)

- transferring software changes, from RISC System/6000 using Xmodem 12-32
- transferring software changes, IBM 6611 diskette 12-26
- transferring software changes, RISC System/6000 diskette 12-27
- Verify a Software Component 12-39
- View History of a Software Component 12-38
- View ID of a Software Component 12-38
- software installation and maintenance facility 12-2
- Software Installation and Maintenance menu 7-31
- software installation procedure 12-6
- software lock 10-57
- software loopback active 6-69
- software loopback active, XNS 6-76
- software operations 10-3
- software problem determination
 - description of 7-23
 - using the performance and statistics facilities 11-54
 - using the System Manager 11-3
- software requirements
 - Configuration Program 2-6
- software update installation procedure 12-9
- software updates 12-2
- software VPD 12-33
- source address mask, SNA 3-29, 3-30
- source address, SNA 3-28, 3-30
- source frame address for outbound filters 6-19
- source frame address mask for outbound filters 6-19
- source frame address mask on SRB port 6-10
- source frame address on SRB port 6-9
- source frame filter type 3-28
- source host value, IPX port 6-73
- source host value, XNS 6-81
- source name filter type, NetBIOS 3-48
- source name, NetBIOS 3-48, 3-49
- source network value, IPX port 6-73
- source network, XNS 6-80
- source route bridging
 - bridge number 3-4
 - bridge priority 3-5
 - designated ring number 3-4
 - enable source route bridging 3-4
 - filter ordering (port level)
 - inbound filters 6-16
 - outbound filters 6-25
 - filter ordering (system level) 3-6
- filters
 - inbound sliding window 6-13
 - outbound sliding window 6-23
- forward delay time 3-5
- hello time 3-5
- introduction 3-4
- maximum age 3-5
- restrictions 3-4
- source SAP on SRB port 6-11
- source SAP value, port SRB 6-21
- source socket value, IPX port 6-74
- source socket value, XNS 6-81
- spanning tree mode 6-6
- spanning tree parameters 3-5
 - BPDU maximum age 3-17
 - bridge priority 3-5, 3-16
 - forward delay 3-16
 - forward delay time 3-5
 - hello time 3-5, 3-16
 - maximum age 3-5
- split horizon for RIP filter, IPX 3-102
- split horizon for RIP filters 3-109
- start using host name service 10-38
- start using time service 10-40
- starting
 - the configuration program on a PS/2 2-6
 - the configuration program on a RS/6000 2-4
- starting the IBM 6611 10-4
- startup counter 5-46
- static directory, exporting files to a remote node 10-52
- static directory, using 10-21
- station address 5-25
- station token-ring destination address 5-26
- station token-ring destination SAP 5-26
- station token-ring source address 5-25
- station token-ring source SAP 5-25
- station XID value 5-26
- status and error codes B-1
- status of all define inbound RIP filters, IPX 3-106
- status of all defined DECnet filters on this port 6-84
- status of all defined inbound SNAP filters on this port 6-11
- status of all defined inbound source SAP filter on this port 6-10
- status of all defined IPX filters on this port 6-69
- status of all defined NetBIOS destination name filters 3-49
- status of all defined NetBIOS source name filters 3-48
- status of all defined outbound MAC address filters on this port 6-18
- status of all defined outbound ring number filters on this port 6-22
- status of all defined outbound RIP filters, IPX 3-107
- status of all defined outbound SNAP filters on this port 6-21
- status of all defined outbound source SAP filters for this port 6-20
- status of all defined ring number filters on this port 6-12
- status of all defined RIP router filter, IPX 3-104
- status of all defined SAP filters 3-102
- status of all defined SNA destination frame filters 3-29
- status of all defined SNA source frame filters 3-27
- status of all defined XNS filters on this port 6-77
- status of all inbound RIP filters, XNS 3-109

- status of all outbound RIP filters 3-111
- status of all RIP router filters 3-112
- stop using host name service 10-38
- stop using time service 10-40
- stopping the IBM 6611 10-4
- stub cost, OSPF 3-52
- subnet mask 6-51
- system address resolution protocol command
 - primitives 8-16
- system configuration
 - baud rate for S1 serial port 4-4
 - baud rate for S2 serial port 4-4
 - domain name 4-3
 - EIA 232 serial ports 4-4
 - IBM 6611 host name 4-3
 - lock value 4-5
 - SNMP 4-6
 - system configuration parameters 3-3
 - system management parameters 4-3
- system configuration changes 10-28
- system configuration information 7-5, 7-6, 10-29, 14-6
- system configuration parameters
 - BGP 3-67
 - data link switching 3-18
 - DECnet 3-115
 - EGP 3-83
 - export filters 3-95
 - Hello 3-63
 - IP over X.25 3-100
 - NetBIOS 3-47
 - OSPF 3-51
 - packet filters 3-92
 - RIP 3-58
 - source route bridging 3-4
 - starting 3-3
 - Static Routes 3-90
 - transparent bridging 3-10
 - XNS 3-109
- system contact 4-7
- system dump command primitives 8-40
- System Environment and Configuration
 - adding a host name to the mapping 10-36
 - adding a name server 10-38
 - adding a time server 10-41
 - adding userids 10-33
 - applying configuration changes to configuration database 10-41
 - changing passwords 10-34
 - changing the date and time 10-26
 - changing the date, time, and time zone 10-27
 - committing configuration changes to configuration database 10-42
 - configuring remote host name service 10-37
 - configuring remote time service 10-39
 - configuring the EIA 232 S1 and S2 serial ports 10-30
 - configuring the host name and domain name 10-34, 10-35

- System Environment and Configuration (*continued*)
 - configuring the host name to IP address mapping 10-34
 - configuring userids and passwords 10-31
 - deleting a host name from the mapping 10-36
 - deleting a name server 10-39
 - deleting a time server 10-41
 - deleting userids 10-33
 - description of 7-28
 - exporting data 10-50
 - exporting files to a remote node 10-52
 - file names in transfer directory 10-43
 - importing data 10-51
 - importing files to a remote node 10-52
 - listing name servers 10-37
 - listing the host name to IP address mapping 10-36
 - listing time servers 10-40
 - listing userids and passwords 10-33
 - performing diskette operations 10-22
 - performing system configuration changes 10-28
 - rejecting configuration changes to configuration database 10-42
 - sending an AT command 10-22
 - start using host name service 10-38
 - start using time service 10-40
 - stop using host name service 10-38
 - stop using time service 10-40
 - using the menu items 10-18
 - using the static directory 10-21
 - using the transfer directory 10-19
 - working with files in the transfer directory 10-19
- System Environment and Configuration menu 7-28
- system location 4-7
- system management parameters
 - address mask 4-18
 - apply configuration 4-19
 - baud rate for S1 serial port 4-4
 - baud rate for S2 serial port 4-4
 - community access 4-15
 - community address 4-14
 - community address mask 4-14
 - community name 4-14
 - community view name 4-15
 - configuration hosts 4-18
 - controlling password 4-16
 - controlling userid 4-16
 - day 4-19
 - description of 4-2
 - domain name 4-3
 - EIA serial ports 4-4
 - enable coldStart trap 4-10
 - enable egpNeighborLoss trap 4-12
 - enable enterpriseSpecific trap 4-12
 - enable linkDown trap 4-11
 - enable linkUp trap 4-11
 - enable name resolution by remote name servers 4-22
 - enable time service by remote time servers 4-23

system management parameters (*continued*)

- enable warmStart trap 4-10
- enterprise-specific trap throttle time 4-8
- host name 4-3, 4-21
- hosts that can perform configuration functions 4-18
- hour 4-20
- IP address 4-18
- IP address of host 4-21
- IP address of name server 4-22
- IP address of remote time server 4-23
- lock/unlocking the Multiprotocol Network Program 4-5
- MIB subtree 4-13
- minute 4-20
- month 4-19
- remote host names 4-21
- router serial number prefix 4-8
- router serial number suffix 4-9
- SNMP 4-6
- system contact 4-7
- system location 4-7
- system name 4-7
- time to perform configuration 4-19
- trap address 4-10
- trap community name 4-10
- userid and passwords 4-16
- view name 4-12
- viewing password 4-17
- viewing userid 4-16
- year 4-19

System Manager tasks

- Adapter and Protocol Configuration 7-36
- Concurrent Hardware Diagnostics 7-25
- Configuration Files and Reports 7-35
- flowchart 7-17
- Hardware Vital Product Data 7-34
- menu screens 7-17
- Performance and Statistics 7-22
- performing 7-16
- Problem Determination Facilities 7-23
- Remote Accesses to Other Nodes 7-30
- Resource Control and Management 7-27
- Software Installation and Maintenance 7-31
- System Environment and Configuration 7-28

System Manager, 6611

- hardware diagnostics 13-2

system name 4-7

system routing table, viewing 10-7

system shutdown command primitives 8-76

system time command primitives 8-89

system trace command primitives 8-91

system user command primitives 8-98

system-level parameters

- AppleTalk 3-101
- APPN 3-32
- data link switching 3-18
- NetBIOS 3-47
- source route bridging 3-4

system-level parameters (*continued*)

- transparent bridging 3-10

- XNS 3-109

Systems Network Architecture

- destination address 3-29, 3-31
- destination address mask 3-29, 3-31
- destination frame filter type 3-30
- filter ID 3-28, 3-30
- IP address of destination router 3-27
- source address 3-28, 3-30
- source address mask 3-29, 3-30
- source frame filter type 3-28
- status of all defined SNA destination frame filters 3-29
- status of all defined SNA source frame filters 3-27

T

T1 timer 5-45

T24 timer 5-46

T25 timer 5-46

T4 timer 5-45

tag, exports 3-99

tasks, performance and statistics

tasks, problem determination

- Clean the Error Log 11-10

- Copy Error Log or Trace Log to Transfer Directory 11-53

- Copy System Dump to Diskette or Transfer Directory 11-14

- Dump Adapter Memory 11-41

- Export Problem Determination Output 11-53

- Extract Error Log Records From System Dump 11-15

- Extract Trace Log Records From System Dump 11-15

- Read Adapter Memory 11-38

- selecting a 11-3

- Set DECnet Trace Output 11-50

- Start Adapter Line Trace 11-39

- Start and Stop SNMP Trace 11-28

- Start AppleTalk Protocol Trace 11-31

- Start APPN Trace 11-34

- Start APPN User Process Memory Dump 11-16

- Start Bridging Frame Trace 11-44

- Start IP Routing Protocols Dump 11-19

- Start IP Routing Protocols Trace 11-25

- Start System Dump 11-12

- Start System Trace 11-21

- Start User Process Memory Dump 11-16

- Stop AppleTalk Protocol Trace 11-32

- Stop APPN Trace 11-35

- Stop Bridging Frame Trace 11-45

- Stop IP Routing Protocols Trace 11-26

- Stop System Trace 11-22

- Use Adapter Debug Facility 11-37

- Use DECnet Debug Facility 11-48

- Use Source Route Bridging Debug Facility 11-42

- tasks, problem determination (*continued*)
 - Use Special User Process Traces 11-24
 - Use System and User Process Dump Facilities 11-11
 - Use System Trace Facility 11-21
 - View a Formatted System Dump 11-14
 - View Adapter Debug Data in Transfer Directory 11-41
 - View Adapter Registers 11-39
 - View an Error Report 11-6
 - View an Error Report for a Single Sequence Number 11-8
 - View AppleTalk Protocol Trace 11-32
 - View APPN Trace Report 11-35
 - View Bridge Configuration Information 11-46
 - View Bridge SAP Filter Information 11-47
 - View Bridge Trace Files 11-44
 - View Bridging Frame Trace Output 11-45
 - View DECnet Trace Output 11-52
 - View IP Routing Protocols Dump 11-19
 - View IP Routing Protocols Trace 11-26
 - View Previous System Dump Information 11-13
 - View Routing Data Structures 11-48
 - View SNMP Trace 11-28
 - View System Monitor Trace 11-29
 - View System Trace Report 11-22
 - View User Process Memory Dump 11-17
 - View X.25 Trace 11-30
- telecommunication link error threshold 5-12
- telnet 9-7, 9-8, 9-12
- third party sales 10-57
- three-digit display, using 10-6
- time and date changes 10-26, 10-27
- time servers 10-39
- time to perform configuration 4-19
- to protocol, exports 3-99
- Token-Ring Adapter parameters
 - broadcast type 5-5
 - compatible protocols 5-3
 - enable interface 5-3
 - introduction 5-3
 - locally administered address 5-4
 - MAC Address 5-3
 - MAC Address Format 5-4
 - token-ring data rate 5-5
- Token-Ring Network 16/4 Adapter 5-3
- Token-Ring Network Bridge Program point-to-point protocol
 - auto reboot on error 5-12
 - enable configuration report saver 5-14
 - enable LAN bridging protocol on this port 5-12
 - enable ring error monitor 5-14
 - enable ring parameter server 5-14
 - event log drive 5-13
 - introduction 5-12
 - largest frame size 5-13
 - link password 0 5-14
 - link password 1 5-15
 - Token-Ring Network Bridge Program point-to-point protocol (*continued*)
 - link password 2 5-15
 - link password 3 5-15
 - memory dump on error 5-13
 - performance counter threshold 5-12
 - restrictions 5-12
 - telecommunication link error threshold 5-12
 - transfer directory file names 10-43
 - transfer directory, exporting data 10-50
 - transfer directory, exporting files to a remote node 10-52
 - transfer directory, importing data 10-51
 - transfer directory, importing files to a remote node 10-52
 - transfer directory, using 10-19
 - transferring files 10-43
 - transferring files to diskette 10-57
 - transferring files, using FTP 10-52
 - transferring files, using modem 10-55
 - transit area ID, OSPF 3-56
 - transmit packet size, SVC 5-48
 - transmit packet window size, PVC 5-39
 - transmit packet window size, SVC 5-48
 - transmit window count 5-28
 - transparent bridging
 - aging time 3-12
 - BPDU maximum age 3-17
 - bridge priority 3-16
 - enable at port 6-29
 - enable transparent bridging 3-11
 - filter ordering (port level)
 - inbound filters 6-39
 - outbound filters 6-47
 - filter ordering (system level) 3-13
 - filtering database parameters 3-12
 - filters
 - inbound Ethernet Type 6-36
 - inbound MAC address 6-33
 - inbound sliding window 6-37
 - inbound source SAP 6-35
 - outbound Ethernet Type 6-43
 - outbound MAC address 6-41
 - outbound sliding window 6-45
 - outbound source SAP 6-43
 - forward delay 3-16
 - hello time 3-16
 - introduction 3-10
 - LLC duplicate address check 3-11
 - MAC address form 3-11
 - maximum transmission unit (frame) size 6-33
 - overflow policy 3-12
 - port-level parameters 6-29
 - restrictions 3-10
 - spanning tree parameters 3-16
 - static destination address filters 3-12, 3-13
 - transport control value, IPX port 6-71

transport control value, XNS 6-79

transporting

configuration file 2-13

trap address, SNMP 4-10

trap community name 4-10

traps

enable coldStart trap 4-10

enable egpNeighborLoss trap 4-12

enable enterpriseSpecific trap 4-12

enable linkDown trap 4-11

enable linkUp trap 4-11

enable warmStart trap 4-10

enterprise-specific trap throttle time 4-8

type of line 5-32

type, exports 3-99

type, IPX 3-103

U

unconfigured neighbor parameters, BGP 3-76

unconfigured neighbor, BGP 3-76

use InARP to resolve remote protocol addresses 5-20

user process dump command primitives 8-42

user process trace command primitives 8-94

user-defined facilities 5-48

userids 9-8, 9-10, 9-13, 9-25

userids and passwords 10-31

using

Active Internet Connection Information 11-81

Bridge Statistics 11-74

Clean the Error Log 11-10

configuration program 2-2

Connection Statistics 11-70, 11-77

Copy Error Log or Trace Log to Transfer
Directory 11-53

Copy System Dump to Diskette or Transfer
Directory 11-14

Dump Adapter Memory 11-41

Export Performance Data 11-89

Export Problem Determination Output 11-53

Extract Error Log Records From System
Dump 11-15

Extract Trace Log Records From System
Dump 11-15

Filter Information 11-73

function keys 7-11

LAN Bridge Internal Protocol Frame
Statistics 11-86

LAN Bridge Statistics 11-75, 11-85

List Process Commands 11-62

List Processes 11-61

Main Window 2-7

Memory Management Statistics 11-80

Packet Traffic Statistics 11-72, 11-79

Protocol Statistics 11-71

Read Adapter Memory 11-38

Set DECnet Trace Output 11-50

Source Route Bridge Spanning Tree Frame Relay
Statistics 11-82

using (*continued*)

Source Route Bridge Spanning Tree

Statistics 11-82

Spanning Tree Statistics 11-82

Start Adapter Line Trace 11-39

Start and Stop SNMP Trace 11-28

Start AppleTalk Protocol Trace 11-31

Start APPN Trace 11-34

Start APPN User Process Memory Dump 11-16

Start Bridging Frame Trace 11-44

Start IP Routing Protocols Dump 11-19

Start IP Routing Protocols Trace 11-25

Start System Dump 11-12

Start System Trace 11-21

Start User Process Memory Dump 11-16

Stop AppleTalk Protocol Trace 11-32

Stop APPN Trace 11-35

Stop Bridging Frame Trace 11-45

Stop IP Routing Protocols Trace 11-26

Stop System Trace 11-22

System Manager screens 7-3

System Socket Information 11-81

TCP/IP Protocol Statistics 11-77

TCP/IP Route Statistics 11-80

Transparent Bridge Spanning Tree Frame Relay
Statistics 11-84

Transparent Bridge Spanning Tree Statistics 11-83

Use Adapter Debug Facility 11-37

Use DECnet Debug Facility 11-48

Use Source Route Bridging Debug Facility 11-42

Use Special User Process Traces 11-24

Use System and User Process Dump
Facilities 11-11

Use System Trace Facility 11-21

View a Formatted System Dump 11-14

View Adapter Debug Data in Transfer
Directory 11-41

View Adapter Interface Statistics 11-69

View Adapter Registers 11-39

View an Error Report 11-6

View an Error Report for a Single Sequence
Number 11-8

View AppleTalk Protocol Trace 11-32

View APPN Trace Report 11-35

View Bridge Configuration Information 11-46

View Bridge SAP Filter Information 11-47

View Bridge Trace Files 11-44

View Bridging Frame Trace Output 11-45

View DECnet Trace Output 11-52

View Input/Output Statistics 11-88

View IP Routing Protocols Dump 11-19

View IP Routing Protocols Trace 11-26

View Network Management Information 11-57

View Previous System Dump Information 11-13

View Process Information 11-63

View Process Information and Status 11-61

View Process Status 11-65

View Process Table Information 11-67

using (*continued*)

- View Protocol and Interface Packet Traffic Information 11-55
 - View Routing Data Structures 11-48
 - View SNMP Trace 11-28
 - View System Activity Report 11-59
 - View System Monitor Trace 11-29
 - View System Network Statistics 11-75
 - View System Trace Report 11-22
 - View User Process Memory Dump 11-17
 - View Virtual Memory Statistics 11-87
 - View X.25 Trace 11-30
- using a modem 9-17, 10-43

V

- V.35 5-22
- verification
 - repair 13-2
- Verify a Software Component 12-39
- View History of a Software Component 12-38
- View ID of a Software Component 12-38
- view name 4-12
- viewing password 4-17
- viewing userid 4-16
- viewing users 9-25
- virtual circuit type 5-47
- virtual link ID 3-56
- virtual neighbor ID, OSPF 3-56
- virtual ring segment number 3-25
- vital product data
 - exporting software 12-40
 - hardware 7-34
 - in the error log 11-5
 - software 7-32, 12-33

W

- warning notice
 - about erasing error log 11-5, 11-10
 - System Manager Configuration 7-36
- working with files 10-43
- worksheets
 - system configuration A-2

X

- X.21 5-22
- X.25
 - compatible protocol 5-30
 - connection decay interval 3-100
 - enable X.25 5-32
 - introduction 5-30
 - local DTE address (NUA) 5-33
 - lowest LCN for 2-way SVC 5-34
 - lowest LCN for outgoing SVCs 5-33
 - network identifier 5-33
 - number of LCNs for outgoing SVCs 5-33
 - restriction 5-30

X.25 (*continued*)

- SVC packet sizes 5-30
- SVC window sizes 5-31
- type of line 5-32
- Xerox Network Systems
 - enable XNS router 3-109
 - filter ID 3-110, 3-111, 3-113
 - filtering mode 3-110, 3-111, 3-112
 - host address 3-113
 - host address to filter on 3-113
 - introduction 3-109
 - local XNS network to filter on 3-110, 3-111
 - network number 3-110, 3-112, 3-113
 - network number to filter on 3-112
 - network numbers to filter on 3-110, 3-113
 - split horizon for RIP filters 3-109
 - status of all inbound RIP filters 3-109
 - status of all outbound RIP filters 3-111
 - status of all RIP router filters 3-112
- Xmodem 10-43, 10-55
 - baud rate 10-30
 - for the configuration file 2-14
 - sending an AT command 10-22
 - transferring files 10-43
 - transferring software changes from RISC System/6000 12-32
 - using RISC System/6000 10-55
 - using Xmodem 10-55
- Xmodem, using RISC System/6000 10-55
- XNS
 - enable XNS router 3-109
 - filter ID 3-110, 3-111, 3-113
 - filtering mode 3-110, 3-111, 3-112
 - host address 3-113
 - host address to filter on 3-113
 - introduction 3-109
 - local XNS network to filter on 3-110, 3-111
 - network number 3-110, 3-112, 3-113
 - network number to filter on 3-112
 - network numbers to filter on 3-110, 3-113
 - split horizon for RIP filters 3-109
 - status of all inbound RIP filters 3-109
 - status of all outbound RIP filters 3-111
 - status of all RIP router filters 3-112

Y

- year 4-19

Z

- zero reserved fields, RIP 3-58
- zone, time, and date changes 10-27



Part Number: 34G2661

Printed in USA

SC30-3559-02

